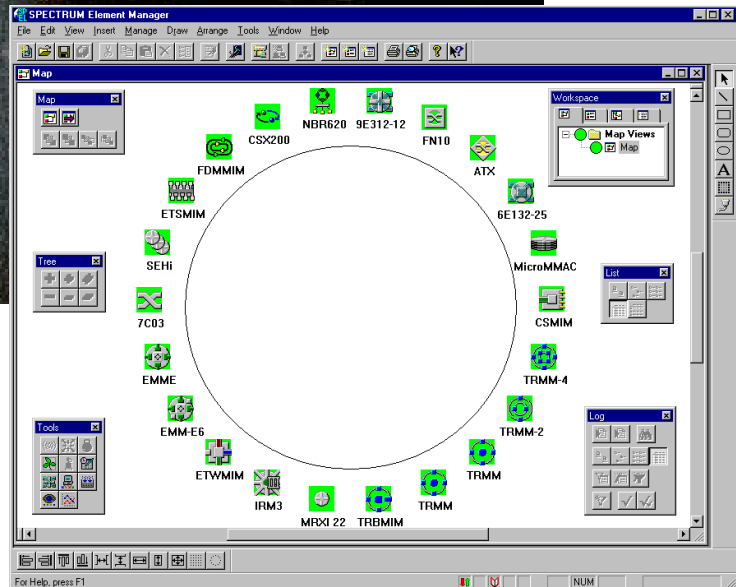
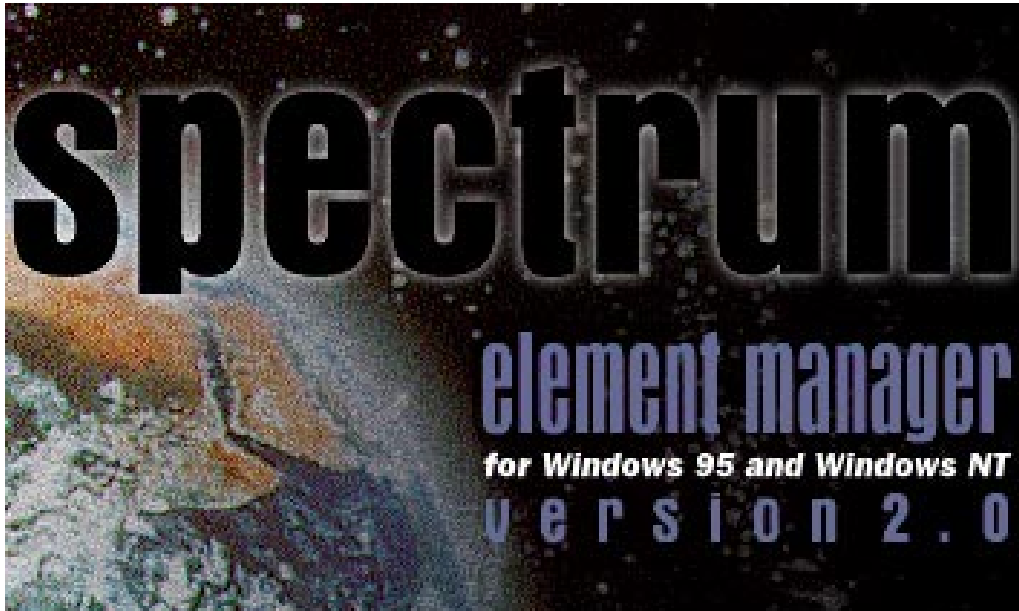


Cabletron Systems



**MMAC-Plus™ Remote Management
for the 9H42x-xx Series
Fast Ethernet SmartSwitch™ Modules**

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © 1997 by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9032074-01 August 1997

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Cabletron Systems, SPECTRUM, BRIM, DNI, FNB, INA, Integrated Network Architecture, LANVIEW, LANVIEW Secure, Multi Media Access Center, MiniMMAC, and TRMM are registered trademarks, and **Bridge/Router Interface Modules, BRIM-A100, CRBRIM-W/E, CRXMIM, CXRMIM, Desktop Network Interface, Distributed LAN Monitoring, Distributed Network Server, DLM, DNSMIM, E1000, E2000, E3000, EFDMMIM, EMM-E6, EMME, EPIM, EPIM-3PS, EPIM-A, EPIM-C, EPIM-F1, EPIM-F2, EPIM-F3, EPIM-T, EPIM-T1, EPIM-X, ESXMIM, ETSMIM, ETWMIM, FDCMIM-04, FDCMIM-08, FDMIM, FDMIM-04, Flexible Network Bus, FOMIM, FORMIM, HubSTACK, IRBM, IRM, IRM-2, IRM-3, Media Interface Module, MicroMMAC, MIM, MMAC, MMAC-3, MMAC-3FNB, MMAC-5, MMAC-5FNB, MMAC-8, MMAC-8FNB, MMAC-M8FNB, MMAC-Plus, MRX, MRXI, MRXI-24, MultiChannel, NB20E, NB25E, NB30, NB35, NBR-220/420/620, RMIM, SecureFast Packet Switching, SFPS, SPECTRUM Element Manager, SPECTRUM for Open Systems, SPIM-A, SPIM-C, SPIM-F1, SPIM-F2, SPIM-T, SPIM-T1, TPMIM, TPMIM-22, TPMIM-T1, TPRMIM, TPRMIM-36, TPT-T, TRBMIM, TRMM-2, TRMMIM, and TRXI** are trademarks of Cabletron Systems, Inc.

AppleTalk, Apple, Macintosh, and TokenTalk are registered trademarks; and Apple Remote Access and EtherTalk are trademarks of Apple Computer, Inc.

SmartBoost is a trademark of American Power Conversion

ST is a registered trademark and C++ is a trademark of AT&T

Banyan and VINES are registered trademarks of Banyan Systems, Inc.

cisco, ciscoSystems, and AGS+ are registered trademarks; and cBus, cisco Router, CRM, IGS, and MGS are trademarks of cisco Systems, Inc.

GatorBox is a registered trademark; and GatorMail, GatorMIM, GatorPrint, GatorShare, GatorStar, GatorStar GX-M, and XGator are trademarks of Cayman Systems, Inc.

CompuServe is a registered trademark of CompuServe Incorporated

X Window System is a trademark of Consortium, Inc.

CTERM, DECnet, and ULTRIX are registered trademarks; and DEC, DEC C++, DECnet-DOS, DECstation, VAX DOCUMENT, VMA, and VT are trademarks of Digital Equipment Corporation

Fore Systems, ForeRunner, and ForeRunner ASX-100 are trademarks of Fore Systems, Inc.

PC/TCP is a registered trademark of FTP Software, Inc.

HP OpenView is a registered trademark of Hewlett-Packard, Inc.

AIX, IBM, OS/2, NetView, and PS/2 are registered trademarks; and AT, Micro Channel, PC, PC-DOS, PC/XT, Personal Computer AT, Operating System/2, Personal System/2, RISC System/6000, and Workplace Shell are trademarks of International Business Machines Corporation

i960 microprocessor is a registered trademark; and Intel and Multichannel are trademarks of Intel Corporation

Microsoft, MS-DOS, and Windows are registered trademarks of Microsoft Corporation

Chameleon, ChameleonNFS, Chameleon 32, IPX/link, and NEWT are trademarks of NETMANAGE, Inc.

NetWare and Novell are registered trademarks; and Internetwork Packet Exchange (IPX), IPX, and Network File System (NFS) are trademarks of Novell, Inc.

Motif and MS are registered trademarks; and Open Software Foundation, OSF, OSF/1, and OSF/Motif are trademarks of The Open Software Foundation, Inc.

Silicon Graphics and IRIS are registered trademarks; and Indigo and IRIX are trademarks of Silicon Graphics, Inc.

NFS, PC-NFS, SPARC, Sun Microsystems, and Sun Workstation are registered trademarks; and OpenWindows, SPARCstation, SPARCstation IPC, SPARCstation IPX, Sun, Sun-2, Sun-3, Sun-4, Sun386i, SunNet, SunOS, SunSPARC, and SunView are trademarks of Sun Microsystems, Inc.

OPEN LOOK and UNIX are registered trademarks of Unix System Laboratories, Inc.

Ethernet, NS, Xerox Network Systems and XNS are trademarks of Xerox Corporation

ANNEX, ANNEX-II, ANNEX-IIe, ANNEX-3, ANNEX-802.5, MICRO-ANNEX-XL, and MICRO-ANNEX-ELS are trademarks of Xylogics, Inc.

MAXserver and Xyplex are trademarks of Xyplex, Inc.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.
 - (b) This computer software may be:
 - (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;
 - (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;
 - (3) Reproduced for safekeeping (archives) or backup purposes;
 - (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;
 - (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and
 - (6) Used or copied for use in or transferred to a replacement computer.
 - (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.
 - (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.
 - (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Chapter 1 Introduction

Using the 9H42x-xx User's Guide	1-3
Related Manuals.....	1-4
Software Conventions	1-4
Common 9H42x-xx Window Fields	1-4
Using Buttons	1-6
Getting Help	1-6
Using On-line Help.....	1-6
Getting Help from Cabletron Systems' Global Call Center	1-7
9H42x-xx Firmware	1-7

Chapter 2 The 9H42x-xx Module View

Viewing Module Information.....	2-2
Front Panel Information.....	2-3
Menu Structure.....	2-4
Port Status Displays.....	2-8
Selecting a Port Status View	2-9
Port Status Color Codes.....	2-11
The Chassis Manager Window	2-11
Viewing the Device Type	2-12
Viewing I/F Summary Information.....	2-13
Interface Performance Statistics/Bar Graphs	2-14
Viewing Interface Detail	2-16
Making Sense of Detail Statistics.....	2-18
Using the Find Source Address Feature	2-18
Managing the Module	2-19
Configuring Ports	2-19
Configuring Standard Ethernet Ports	2-20
Configuring Fast Ethernet Ports.....	2-21
Setting the Desired Operational Mode.....	2-24
Setting the Device Date and Time	2-25
Enabling and Disabling Ports	2-26

Chapter 3 Alarm Configuration

About RMON Alarms and Events.....	3-1
Basic Alarm Configuration	3-2
Accessing the Basic Alarm Configuration Window.....	3-3
Viewing Alarm Status	3-4

Creating and Editing a Basic Alarm	3-6
Disabling a Basic Alarm	3-9
Viewing the Basic Alarm Log	3-9
Advanced Alarm Configuration	3-11
Accessing the RMON Advanced Alarm/Event List.....	3-11
Creating and Editing an Advanced Alarm.....	3-14
Creating and Editing an Event.....	3-20
Adding Actions to an Event	3-23
Deleting an Alarm, Event, or Action	3-26
Viewing an Advanced Alarm Event Log.....	3-26
How Rising and Falling Thresholds Work	3-27

Chapter 4 Statistics

Accessing the Statistics Windows	4-1
RMON Statistics	4-2
Viewing Total, Delta, and Accumulated Statistics.....	4-5
Printing Statistics	4-6
Interface Statistics.....	4-6

Chapter 5 Bridging

Bridging Basics	5-1
More on Transparent Bridging	5-2
An Overview of Bridge Management	5-2
The Bridge Status Window	5-3
Accessing Other Management Options from the Bridge Status Window	5-5
Enabling and Disabling Bridging	5-6
Enabling and Disabling Individual Interfaces	5-6
Enabling and Disabling All Installed Interfaces	5-6
Bridge Statistics	5-7
Performance Graphs.....	5-7
Configuring the Bridge Performance Graphs.....	5-9
Using Source Addressing	5-10
Altering the Ageing Time	5-10
Bridge Spanning Tree.....	5-11
Viewing Spanning Tree Parameters	5-12
Bridge-level Parameters.....	5-13
Port-specific Parameters	5-15
Changing Bridge Spanning Tree Parameters	5-16
Changing Bridge Priority	5-16
Changing the Spanning Tree Algorithm Protocol Type	5-17
Changing Hello Time	5-17
Changing Max Age Time	5-17
Changing Forwarding Delay Time.....	5-18
Changing Port Priority.....	5-18
Changing Path Cost.....	5-18

Filtering Database	5-19
Configuring the Filtering Database.....	5-22
Altering the Ageing Time	5-23
Changing the Type of Entry	5-23
Changing the Receive Port	5-23
Changing the Port Filtering Action.....	5-24
Adding or Deleting Individual Entries	5-24
Clearing All Permanent, Static, or Dynamic Entries	5-25
Configuring Duplex Modes.....	5-25

Index

Introduction

How to use this guide; related guides; software conventions; getting help; 9H42x-xx firmware versions

Welcome to the Cabletron Systems *MMAC-Plus Remote Management for the 9H42x-xx Series Fast Ethernet SmartSwitch™ Modules User's Guide*. We have designed this guide to serve as a simple reference for using SPECTRUM Element Manager for the 9H42x-xx family of Fast Ethernet SmartSwitch Modules for the MMAC-Plus. These modules provide Fast Ethernet connectivity to the Internal Network Bus (INB) backplane via high-speed packet switching, as well as RMON management, Broadcast Storm Protection, and upcoming SecureFast Virtual Networking features.

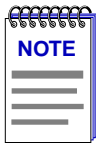
The information presented in this guide covers the following 9H42x-xx devices:

- The **9H421-12** module provides 12 fixed multi-mode fiber 100 Mbps interfaces, each with SC connectors.
- The **9H422-12** module provides 11 fixed 10/100 RJ-45 connections for category 5 twisted pair, and one media-flexible interface designed to accept a Fast Ethernet Port Interface Module (FEPIM). Two Fast Ethernet port modules are available: the FE-100FX, which provides a single multi-mode fiber port with an SC connector; and the FE-100TX, with a single Category 5 UTP RJ45 connector.
- The **9H423-26** module provides 24 fixed 10/100 interfaces via two RJ71 connectors, and two fixed multi-mode fiber interfaces, each with SC connectors. Support for this device is beta-quality only.
- The **9H423-28** module provides 28 ports of mixed 10/100 connectivity: 24 standard Ethernet (10Mbps) interfaces via two RJ71 connectors; two 10/100 interfaces via two fixed RJ45 connectors; one fixed multi-mode fiber Fast Ethernet interface (with an SC connector); and one slot for an FEPIM module.
- And finally, the **9H429-12** module provides 12 fixed single-mode fiber Fast Ethernet interfaces, also with SC connectors.

Each front-panel port (regardless of media type or bandwidth capability) can be configured to operate in Full Duplex Switched Ethernet (FDSE) mode. FDSE allows for each 10BaseT port to provide dedicated 20-Mbps bandwidth for connections to file servers or high-end workstations, while 100BaseTX or 100BaseFX ports can be used to deploy fault-tolerant 200-Mbps backbone links. All 100BaseTX ports also support auto-negotiation.

The 9H42x-xx modules support two types of packet switching:

- *Traditional switching*, which is 802.1d bridging based on physical layer address information; it enhances the overall reliability of the network and, with DEC Spanning Tree support, protects against loop conditions.
- *SecureFast™ switching*, which is high-performance switching based on source and destination MAC (physical) layer addresses. Packets received from a source address on a module's protocol-dependent front panel network are converted into fixed-length, protocol-independent packets for transmission across a backplane, and then are re-converted at the destination device into the appropriate physical frame format for reception by the destination address. Future firmware and management software enhancements will allow an administratively defined connection-policy between end stations connected to SecureFast Packet Switching devices.



Firmware support for the SecureFast Virtual Networking (SFVN) feature of the 9H42x-xx family (which allows switching configuration on a per-user level) is in the early stages of release as this document is published; SFVN remote management will be included in a future release of SPECTRUM Element Manager.

Each module also provides a single backplane interface to the INB bus, for common transmission of data with all other modules of any media connected to the INB in the chassis. The INB is the Cabletron-proprietary network bus for protocol-independent, high-speed packet or cell switching between connectivity modules that support front-panel Ethernet, FDDI, Token Ring, or ATM networks. The connectivity modules incorporate Cabletron's SecureFast Switch (SFS) technology to provide high-performance packet switching based on source and destination MAC addresses, rather than on internet protocol (IP) addresses. By basing packet switching on physical layer information, the INB allows your network infrastructure to be protocol independent. The INB backplane consists of two channels (INB-1 and INB-2), each featuring a 64-byte wide data path capable of a sustained data transfer rate of 2 Gigabits/second (4 Gigabits/second for the combined channels); all 9H42x-xx modules connect to INB-2. The INB backplane requires no management, as its data transmission is subject to hardware defaults.

Using the 9H42x-xx User's Guide

Remote management for the 9H42x-xx family of modules is available from two main resources: the MMAC-Plus Chassis View application, which displays and provides management for an MMAC-Plus chassis (and its installed modules); and the individual Module Views, which provide management for single modules. This guide contains information about software functions accessed directly from an individual Module View; for information about monitoring and controlling a configured MMAC-Plus chassis, see the *Using MMAC-Plus Remote Management User's Guide* included with your software. Additional management information about tools and features common to many devices can also be found in the *Installing and Using SPECTRUM Element Manager* guide, the *SPECTRUM Element Manager Tools Guide*, and the *Remote Administration Tools User's Guide*.

Note that, since the management functionality available for each module in the 9H42x-xx family is virtually identical, the modules will be referred to collectively here as the 9H42x-xx.

This manual contains the following information:

Chapter 1, **Introduction**, provides a list of related documentation, describes certain software conventions, and shows you how to contact Cabletron Systems' Global Call Center.

Chapter 2, **The 9H42x-xx Module View**, describes the visual display of the 9H42x-xx modules and explains how to use the mouse within the Module View; the operation of several module-level management functions — such as changing the module display, enabling and disabling ports, and setting device date and time — is also described here.

Chapter 3, **Alarm Configuration**, provides instructions for using both the Basic and Advanced alarm applications to configure both alarms and the events that notify you that an alarm condition has occurred. The ability to automatically initiate a SET or a series of SETs in response to an alarm — functionality provided by Cabletron's proprietary Actions MIB — is also described.

Chapter 4, **Statistics**, describes the two statistics views available at the interface level: MIB-II Interface statistics, and RMON statistics.

Chapter 5, **Bridging**, provides a comprehensive look at all management options associated with the traditional switching — or bridging — functionality currently available on all front panel interface ports, including Bridge Performance Graphs, Spanning Tree, and the Filtering Database.

We assume that you have a general working knowledge of Ethernet and Fast Ethernet IEEE 802.3 type data communications networks and their physical layer components, and that you are familiar with general bridging and switching concepts.

Related Manuals

The *MMAC-Plus Remote Management for the 9H42x-xx Series Fast Ethernet SmartSwitch Modules User's Guide* is only part of a complete document set designed to provide comprehensive information about the features available to you through SPECTRUM Element Manager. Other guides which include important information related to managing the 9H42x-xx modules include:

Cabletron Systems' *Using MMAC-Plus Remote Management Guide*

Cabletron Systems' *Installing and Using SPECTRUM Element Manager Guide*

Cabletron Systems' *SPECTRUM Element Manager Tools Guide*

Cabletron Systems' *SPECTRUM Element Manager Remote Administration Tools User's Guide*

Cabletron Systems' *SPECTRUM Element Manager Remote Monitoring (RMON) User's Guide*

Cabletron Systems' *Network Troubleshooting Guide*

Microsoft Corporation's *Microsoft Windows User's Guide*

For more information about the capabilities of the 9H42x-xx modules, consult the appropriate hardware documentation.

Software Conventions

SPECTRUM Element Manager's device user interface contains a number of elements which are common to most windows and which operate the same regardless of which window they appear in. A brief description of some of the most common elements appears below; note that the information provided here is not repeated in the descriptions of specific windows and/or functions.

Common 9H42x-xx Window Fields

Similar descriptive information is displayed in boxes at the top of most device-specific windows in SPECTRUM Element Manager, as illustrated in [Figure 1-1](#).

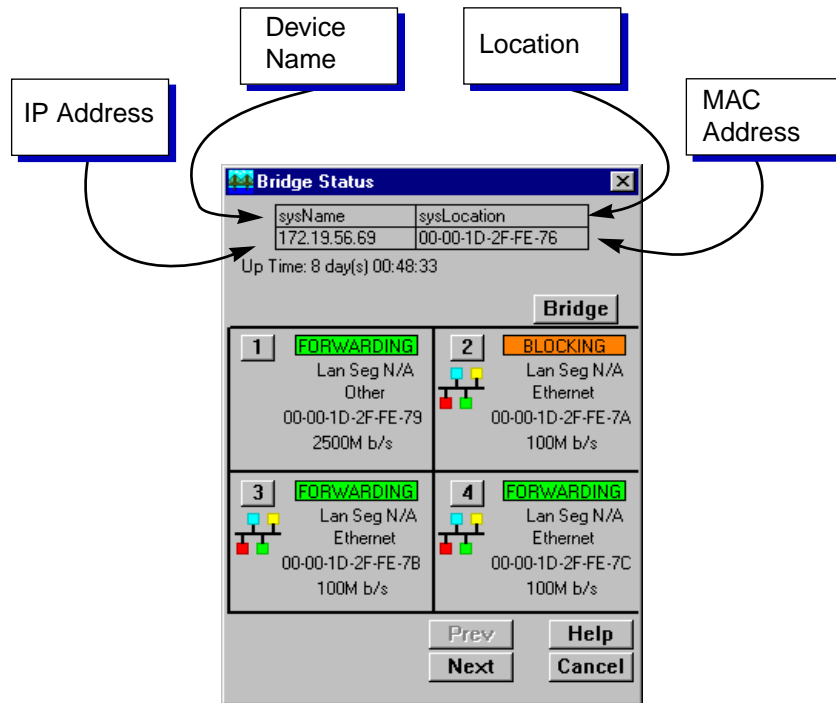


Figure 1-1. Sample Window Showing Informational Text Boxes

Device Name

Displays the user-defined name of the device. The device name can be changed via the System Group window; see the *Generic SNMP Management Module Guide* for details.

IP Address

Displays the device's IP (Internet Protocol) Address; this will be the IP address used to define the device icon. The IP address is assigned via Local Management, and cannot be changed via SPECTRUM Element Manager. Note that although each interface on a 9H42x-xx module has its own MAC, or physical, address, only a single IP address is assigned.

Location

Displays the user-defined location of the device. The location is entered through the System Group window; see the *Generic SNMP Guide* for details.

MAC Address

Displays the manufacturer-set MAC address of the interface through which SPECTRUM Element Manager is communicating with the 9H42x-xx module (typically the SMB10 backplane management interface). MAC addresses are factory-set and cannot be altered.

Using Buttons

The **Cancel** button that appears at the bottom of most windows allows you to exit a window and terminate any unsaved changes you have made. You may also have to use this button to close a window after you have made any necessary changes and set them by clicking on an **OK**, **Set**, or **Apply** button.

An **OK**, **Set**, or **Apply** button appears in windows that have configurable values; it allows you to confirm and SET changes you have made to those values. In some windows, you may have to use this button to confirm each individual set; in other windows, you can set several values at once and confirm the sets with one click on the button.

The **Help** button brings up a Help text box with information specific to the current window. For more information concerning Help buttons, see **Getting Help**, page 1-6.

The command buttons (for example **Bridge**) call up a menu listing the windows, screens, or commands available for that topic.

Any menu topic followed by ... (three dots) — for example, **Statistics...** — calls up a window or screen associated with that topic.

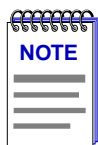
Getting Help

This section describes different methods of getting help for questions or concerns you may have while using SPECTRUM Element Manager.

Using On-line Help

You can use the 9H42x-xx module window **Help** buttons to obtain information specific to the device. When you click on a Help button, a window will appear which contains context-sensitive on-screen documentation that will assist you in the use of the windows and their associated command and menu options. Note that if a Help button is grayed out, on-line help has not yet been implemented for the associated window.

From the **Help** menu accessed from the Module View window menu bar, you can access on-line Help specific to the Module View, as well as bring up the Chassis Manager window for reference. Refer to **Chapter 2** for information on the Module View and Chassis Manager windows.



*All of the SPECTRUM Element Manager help windows use the standard Microsoft Windows help facility; if you are unfamiliar with this feature of Windows, you can select **Help** → **How to Use Help** from the primary window menu bar, or consult your Microsoft Windows **User's Guide**.*

Getting Help from Cabletron Systems' Global Call Center

If you need support related to SPECTRUM Element Manager, or if you have any questions, comments, or suggestions related to this manual or any of our products, please feel free to contact Cabletron Systems' Global Call Center via one of the following methods:

By phone:	Monday through Friday between 8 AM and 8 PM Eastern Standard Time at (603) 332-9400
By mail:	Cabletron Systems, Inc. PO Box 5005 Rochester, NH 03866-5005
By Internet mail:	support@ctron.com
By FTP	ftp.ctron.com (134.141.197.25)
<i>Login</i>	anonymous
<i>Password</i>	your email address
By BBS:	(603) 335-3358
<i>Modem Setting</i>	8N1: 8 data bits, 1 stop bit, No parity

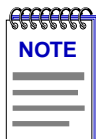
For additional information about Cabletron Systems products, visit our World Wide Web site: <http://www.cabletron.com/>. For Technical Support, select **Service and Support**.

9H42x-xx Firmware

SPECTRUM Element Manager support for the 9H42x-xx series of MMAC-Plus SmartSwitches has been tested against the following firmware versions:

- 9H421-12: version 1.07.06
- 9H422-12: version 1.04.11
- 9H423-28: version 1.05.04
- 9H429-12: version 1.04.10

The 9H423-26 has not yet been customer-released; management support for this device is beta quality.



As a general rule, firmware versions for new products are liable to change rapidly; contact Cabletron Systems' Global Call Center, your local sales representative, or our Web site for upgrade information for the latest customer release of firmware.


The 9H42x-xx Module View

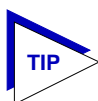
Accessing the Module View; information displayed in the Module View window; the Chassis Manager window; module management functions; port configuration

The Module View window is the main screen that immediately informs you of the status of the front panel interfaces and the INB backplane connection on your 9H42x-xx module via a color-coded, graphical display. The Module View window serves as a single point of access to all management functions available for an individual 9H42x-xx module.

You can launch the 9H42x-xx module view directly from an individual device icon, or from within an MMAC-Plus Chassis view:

from an individual device icon:

1. In any map, list, or tree view, double-click on the 9H42x-xx module you wish to manage;
- or**
1. In any map, list, or tree view, click the **left** mouse button once to select the module you wish to manage.
 2. Select **Manage**—>**Node** from the primary window menu bar, or select the Manage Node  toolbar button.
- or**
1. In any map, list, or tree view, click the **right** mouse button once to select the module you wish to manage.
 2. On the resulting menu, click to select **Manage**.



*To successfully launch the Module View in the above ways, you must have selected either **Chassis Manager** or **User Selectable** as the default MMAC-Plus Startup Option. You set these options via the **Node** page in the **Tools**—>**Options** window; see your **Installing and Using** guide for more details.*

from the MMAC-Plus Chassis View:

1. Click the **left** mouse button on the index number for the slot which contains the 9H42x-xx module you wish to manage.
2. On the resulting menu, click to select **Device View**.

The 9H42x-xx Module View, illustrated in [Figure 2-1](#), will appear.

Viewing Module Information

The Module View window ([Figure 2-1](#)) provides a graphic representation of the 9H42x-xx Module, including a color-coded port display which immediately informs you of the current configuration and status of the module and its ports. Note that the Module View display is essentially the same for all 9H42x-xx modules; the only difference is the number of front panel interfaces.

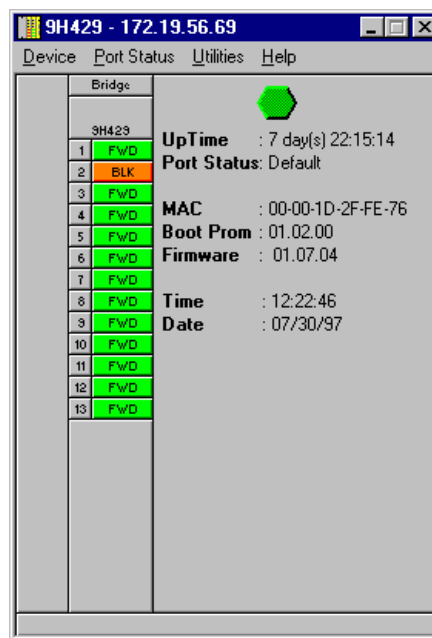
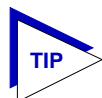
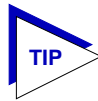



Figure 2-1. 9H42x-xx Module View Window



For the 9H423-26 and 9H423-28 modules, the interface display will include arrows at the top and bottom; these allow you to shift the port display so that you can view the status of and access management for all available ports.

By clicking in designated areas of the module's graphical display (as detailed later in this chapter), or by using the menu bar at the top of the Module View window, you can access all of the menus that lead to more detailed device- and port- level windows.



When you move the mouse cursor over a management "hot spot" the cursor icon will change into a "hand"  to indicate that clicking in the current location will bring up a management option.

Front Panel Information

The areas above and to the right of the main module display area provide the following device information:

IP

The Module View window title displays the device's IP (Internet Protocol) Address; this will be the IP address you have used to create the 9H42x-xx module in the Chassis Setup window, or the IP address used to define the device icon. The IP address is assigned via Local Management, and cannot be changed via SPECTRUM Element Manager. Note that although each interface on the 9H42x-xx module has its own MAC, or physical, address, only a single IP address is assigned.

Connection Status



This color-coded area indicates the current state of communication between SPECTRUM Element Manager and the 9H42x-xx module:

- **Green** indicates the 9H42x-xx is responding to device polls (valid connection).
- **Magenta** indicates that the 9H42x-xx is in a temporary stand-by mode while it responds to a physical change in the hub (such as when a board is inserted); note that board and port menus are inactive during this stand-by state.
- **Blue** indicates an unknown contact status — polling has not yet been established with the 9H42x-xx module.
- **Red** indicates the 9H42x-xx module is not responding to device polls (device is off line, or device polling has failed across the network for some other reason).

Up Time

The amount of time, in a day(s) hh:mm:ss format, that the 9H42x-xx Module has been running since the last start-up.

Port Status

Indicates the Port Status display selection currently in effect. The default port status view is bridge status; if you have not changed the port status selection since launching the Module View window, this field will display **Default**. For more information about changing the port status display, see [page 2-8](#).

MAC

The physical layer address assigned to the interface through which SPECTRUM Element Manager is communicating with the 9H42x-xx Module. Unless your management station is communicating through the front panel of the module, this will reflect the MAC address of the SMB 10 backplane management interface. MAC addresses are hard-coded in the device, and are not configurable.

Boot Prom

The revision of BOOT PROM installed in the 9H42x-xx module.

Firmware

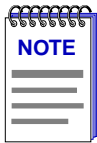
The revision of device firmware stored in the 9H42x-xx module's FLASH PROMs.

Time

The current time, in a 24-hour hh:mm:ss format, set in the 9H42x-xx module's internal clock.

Date

The current date, in an mm/dd/yy format, set in the 9H42x-xx module's internal clock.



You can set the date and time by using the *Edit Device Date* and *Edit Device Time* options on the Device menu; see *Setting the Device Date and Time*, [page 2-25](#), for details.

Menu Structure

By clicking on various areas of the Module View display, you can access menus with bridging configuration and performance options, as well as utility applications and general device management functions. The following illustration displays the menu structure and indicates how to use the mouse to access the various menus:

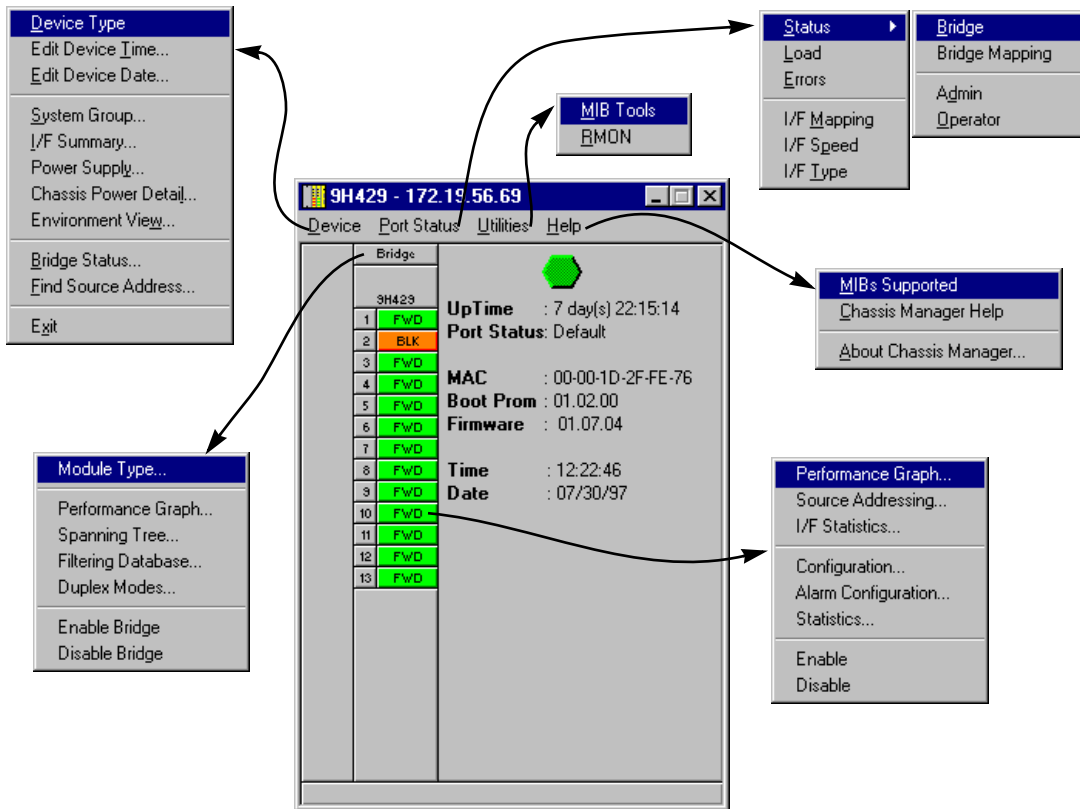


Figure 2-2. 9H42x-xx Module View Menu Structure

The Device Menu

From the Device Menu at the Module View window menu bar, you can access the following selections:

- **Device Type...**, which displays a window containing a description of the device being modeled.
- **Edit Device Time...** and **Edit Device Date...**, which allow you to set the 9H42x-xx module’s internal clock.
- **System Group...**, which allows you to manage the 9H42x-xx module via SNMP MIB II. Refer to the *Generic SNMP User’s Guide* for further information.
- **I/F Summary**, which lets you view statistics (displayed both graphically and numerically) for the traffic processed by each network interface on your device. See **Viewing I/F Summary Information**, page 2-13, for details.

- **Power Supply, Chassis Power Detail, and Environment View** provide access to windows which provide information about the MMAC-Plus chassis the selected module is installed in. A detailed description of these windows can be found in the *Using MMAC-Plus Remote Management User's Guide* included with your software.
- **Bridge Status...**, which opens a window that provides an overview of bridging information for each port, and allows you to access all other bridge-related options. Refer to Chapter 5, **Bridging**, for more information.
- **Find Source Address...**, which opens a window that allows you to search the 9H42x-xx's 802.1d Filtering Database to determine which switching interface a specified source MAC address is communicating through. If the MAC address is detected as communicating through the switch, the port display will flash to indicate the switch interface of interest.
- **Exit**, which closes the 9H42x-xx Module View window.

The Port Status Menu

The Port Status menu allows you to select the status information that will be displayed in the port text boxes in the Module View window:

- **Status** allows you to select one of four status type displays: Bridge, Bridge Mapping, Admin, or Operator.
- **Load** will display the portion of network load processed per polling interval by each interface, expressed as a percentage of the theoretical maximum load (10 or 100 Mbits/sec).
- **Errors** allows you to display the number of errors detected per polling interval by each interface, expressed as a percentage of the total number of valid packets processed by the interface.
- **I/F Port Mapping** will display the interface (if) index associated with each port on your 9H42x-xx module.
- **I/F Speed** will display the port's bandwidth: 10 or 100 Mbits/sec. Note that the module's backplane INB interface has a bandwidth of 2500 Mbits/sec.
- **I/F Type** will display the interface type of each port on the 9H42x-xx module: Eth (ethernet) for all front-panel interfaces, and Other for the backplane INB interface.

For more information on the port display options available via this menu, see [Port Status Displays, page 2-8](#).

The Utilities Menu

The Utilities menu provides access to two important utilities provided by SPECTRUM Element Manager for use with the 9H42x-xx modules: the MIB Tools utility, which provides direct access to the 9H42x-xx module's MIB information; and the RMON utility, a remote monitoring utility which is implemented by many of Cabletron Systems' intelligent devices. These selections are also available from the **Tools** menu in the primary window menu bar.

Refer to your *SPECTRUM Element Manager Tools Guide* for information on the MIB Tools utility, and to the *SPECTRUM Element Manager Remote Monitoring (RMON) User's Guide* for more information on the RMON tool.

The Help Menu

The Help Menu has three selections:

- **MIBS Supported**, which brings up the Chassis Manager window, described on [page 2-11](#).
- **Chassis Manager Help**, which brings up a help window with information specifically related to using the Chassis Manager and Module View windows.
- **About Chassis Manager...**, which brings up a version window for the Chassis Manager application in use.

The Bridge Menu

The Bridge menu is available by clicking on the Bridge label above the port display; it offers access to the following bridge-specific options, which are discussed in detail in Chapter 5, **Bridging**:

- **Module Type...**, which displays a window containing a description of the device being modeled; this is the same information displayed in the Device Type window available from the Device menu. See **Viewing the Device Type**, [page 2-12](#).
- **Performance Graph...**, which visually displays the combined performance of all bridging interfaces on the selected module; see Chapter 5, **Bridging**.
- **Spanning Tree...**, which allows you to set bridge parameters related to the Spanning Tree Algorithm (STA) – the method that bridges use to decide the controlling (root) bridge when two or more bridges are in parallel. See Chapter 5, **Bridging**, for more information.
- **Filtering Database...**, which displays a window to configure the bridge's acquired and permanent filtering databases used to filter or forward traffic across the 9H42x-xx module.
- **Duplex Modes...**, which allows you to set the Duplex Mode for each interface on the module.
- **Disable/Enable Bridge**, which enables or disables bridging across every interface on the module.

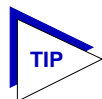
The Port Menu

The menu for the INB and Ethernet interfaces offers the following selections:

- **Performance Graph...**, which brings up a bridging statistics window specific to the selected interface.
- **Source Addressing....**, which brings up a window allowing you to see which source addresses are communicating through the selected switch port when it is using 802.1d bridging. See **Using Source Addressing** in Chapter 5 for more information.
- **I/F Statistics...**, which provides direct access to MIB-II interface statistics for the selected interface. Note that this window may also appear in response to the **Statistics** selection described below, if the RMON MIB component has been disabled for the selected module. See Chapter 4, **Statistics**, for more information.
- **Configuration...**, which allows you to set the duplex mode for standard Ethernet and 100Base-FX fiber interfaces, or configure auto-negotiation parameters for any 100Base-TX interfaces. See **Configuring Ports**, [page 2-19](#), for more information; note that this option is not available for the INB backplane interface.
- **Alarm Configuration...**, which brings up windows that allow you to configure RMON-based alarms and events for each interface; see Chapter 3, **Alarm Configuration**, for details.
- **Statistics...**, which launches the highest level of statistics currently available for the selected interfaces. For all front panel interfaces (both standard Ethernet and Fast Ethernet), RMON statistics will be displayed if the RMON Default MIB component is active; if it has been disabled, MIB-II interface statistics will display. See Chapter 4, **Statistics**, for more information.
- **Enable** and **Disable**, which let you enable or disable bridging across the selected interface; see **Enabling and Disabling Ports**, [page 2-26](#).

Port Status Displays

When you open the Module View window, each port will display its current bridging state (defined below); to change this status display, select one of the options on the Port Status menu, as described in the following sections.



For all 9H42x-xx modules, the port text box indexed "1" indicates the fixed interface to the INB-2 backplane bus; interfaces indexed "2" through "xx" indicate the front panel switching interfaces.

Selecting a Port Status View

To change the status view of your ports:

1. Click on **Port Status** on the menu bar at the top of the Module View window; a menu will appear.
2. Drag down (and to the right, if necessary) to select the status information you want to display. The port text boxes will display the appropriate status information.

Port status view options are:

Status

You can view four port status categories, as follows:

- **Bridge** — FWD, DIS, LRN, LIS, BLK, or BRK
- **Bridge Mapping**
- **Admin** — ON or OFF
- **Operator** — ON or OFF

If you have selected the **Bridge** status mode, a port is considered:

- FWD (Forwarding) if the port is on-line and ready to forward packets across the 9H42x-xx from one network segment to another. Note that this is also the default display for ports which are administratively enabled but not connected.
- DIS (Disabled) if bridging at the port has been disabled by management; no traffic can be received or forwarded on this port, including configuration information for the bridged topology.
- LIS (Listening) if the port is not adding information to the filtering database. It is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.
- LRN (Learning) if the Forwarding database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change. The port is monitoring network traffic, and learning network addresses.
- BLK (Blocking) if the port is on-line, but filtering traffic from going across the 9H42x-xx from one network segment to another. Bridge topology information will be forwarded by the port.
- BRK (Broken) if the physical interface has malfunctioned.

If you have selected **Bridge Mapping**, the port status boxes will display the *bridge* interface index numbers assigned to each interface (which may or may not match the *ifIndex* values displayed via the **I/F Mapping** option described below).

If you have selected the **Admin** status mode, a port is considered:

- ON if the port is enabled by management.
- OFF if it has been disabled through management action.

Note that the Admin state reflects the state *requested* by management; depending on the circumstances, this may or may not match the current Operator status, described below.

If you have selected the **Operator** status mode, a port is considered:

- ON if the port is currently forwarding packets.
- OFF if the port is not currently forwarding packets.

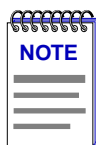
Note that the Operator status provides the *actual* status of the port; depending on the circumstances, this may or may not reflect the Admin state currently *requested* by management. For example, ports which are administratively ON but not yet connected would display an Operator status of OFF, since no packets are being forwarded.

Load

If you choose **Load**, the interface text boxes will display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbits/sec) of the connected network.

Errors

If you choose the **Errors** mode, the interface boxes will display the percentage of the total number of valid packets processed by each port during the last polling interval that were error packets. This percentage reflects the number of errors generated during the last polling interval by devices connected to that port compared to the total number of valid packets processed by the port.



*In SPECTRUM Element Manager, the polling interval is set using the **Tools**—>**Options** window available from the primary window menu bar, or via the individual device icon's Properties window. Refer to the **Installing and Using SPECTRUM Element Manager** guide for full information on setting device polling intervals.*

I/F Mapping

If you choose the I/F Mapping mode, the interface boxes will display the interface number (IfIndex) associated with each port on the 9H42x-xx module. Note that this value may or may not correspond to the *bridge* port index displayed via the **Bridge Mapping** option (described above).

I/F Speed

If you choose the I/F Speed mode, the interface boxes will display the bandwidth of each individual interface on the 9H42x-xx module: 10M (megabits) for standard Ethernet; 100M for Fast Ethernet; and 2500M for the INB backplane interface.

I/F Type

If you choose the I/F Type mode, the interface boxes will display the network type supported by each interface on the 9H42x-xx module: Eth (ethernet-csmacd) or Other (for the INB backplane interface). Note that there is no type distinction between standard Ethernet and Fast Ethernet.

Port Status Color Codes

Three of the Port Status display options — Bridge, Admin, and Operator — incorporate their own color coding schemes: for the Bridge option, green = FWD, blue = DIS, magenta = LIS or LRN, orange = BLK, and red = BRK; for Admin and Operator, green = ON, red = OFF, and blue = N/A (not available).

For all other Port Status selections — Bridge Mapping, Load, Errors, I/F Mapping, I/F Speed, and I/F Type — color codes will continue to reflect the most recently-selected mode which incorporates its own color coding scheme.

The Chassis Manager Window

Like most networking devices, Cabletron's devices draw their functionality from a collection of proprietary MIBs and IETF RFCs. In addition, Cabletron's newer intelligent devices — like the 9H42x-xx module — organize their MIB data into a series of "components." A MIB component is a logical grouping of MIB data, and each group controls a defined set of objects. For example, 9H42x-xx bridging information is organized into its own component; more generic device and port information resides in the chassis component. Note, too, that there is no one-to-one correspondence between MIBs and MIB components; a single MIB component might contain objects from several different proprietary MIBs and RFCs.

The Chassis Manager window, [Figure 2-3](#), is a read-only window that displays the MIBs and the MIB components — and, therefore, the functionality — supported by the currently monitored device.

The MIBs which provide the 9H42x-xx module's functionality — both proprietary MIBs and IETF RFCs — are listed here

MIB Components are listed here; remember, there's no one-to-one correspondence between MIBs and MIB Components

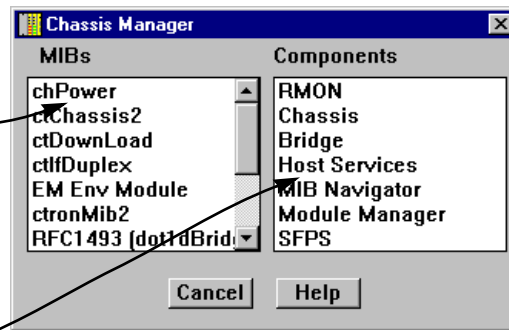


Figure 2-3. Chassis Manager Window

To view the Chassis Manager window:

1. Click on **Help** on the menu bar at the top of the Module View window.
2. Click again to select **MIBs Supported**, and release.

Viewing the Device Type

In addition to the graphical displays described above, the **Device Type** option on the Device menu and the **Module Type** option on the Bridge menu bring up windows that list the physical characteristics of the 9H42x-xx module and its ports:

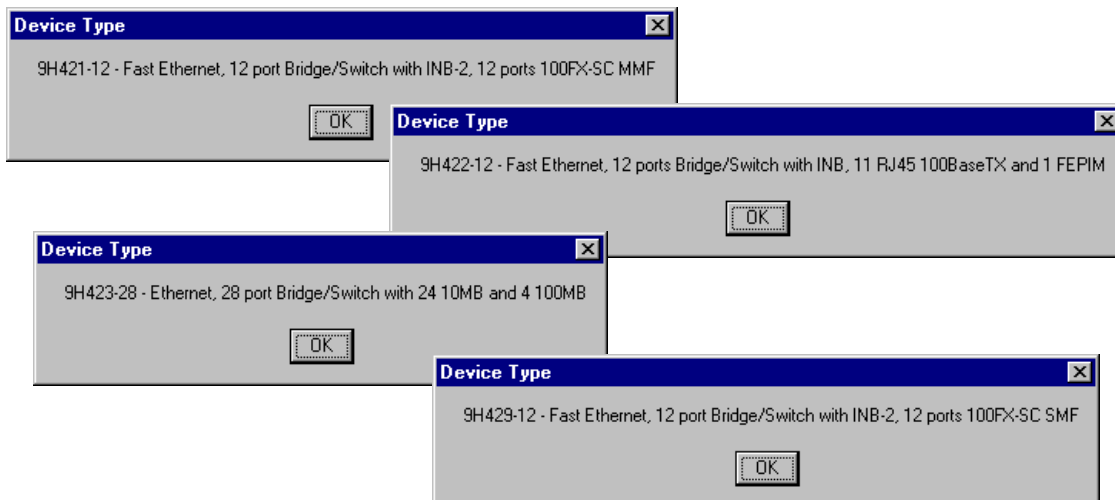


Figure 2-4. Sample Device Type Windows

Viewing I/F Summary Information

The **I/F Summary** menu option available from the Device menu lets you view statistics (displayed both graphically and numerically) for the traffic processed by each network interface on your device. The window also provides access to a detailed statistics window that breaks down Transmit and Receive traffic for each interface; in addition, an **Applications** button in the I/F Summary window lets you access SNMP MIB-II windows for device management.

To access the I/F Summary window:

1. From the Module View, click on the **Device** option from the menu bar.
2. Click again to select **I/F Summary**, and release. The I/F Summary window, [Figure 2-5](#), will appear.

Index	Type	Description	P.Sta	L.Sta	In Octets	Load
1	sdlc	SMB 1	Online	Up		0.14 %
2	ethernet-csmacd	SMB 10	Online	Up		0.00 %
3	Other	HOST	Online	Up		0.03 %
4	Other	HOST	Online	Up		0.03 %
5	Other	INB	Online	Up		0.11 %
6	ethernet-csmacd	Ethernet	Offline	Up		0.00 %
7	ethernet-csmacd	Ethernet	Offline	Up		0.00 %

Figure 2-5. I/F Summary Window

The I/F Summary window provides a variety of descriptive information about each interface on your device, as well as a bar graph and statistics which display each interface's performance.

The following descriptive information is provided for each interface:

UpTime

The **UpTime** field lists the amount of time, in a days, hh:mm:ss format, that the device has been running since the last start-up

Index

The index value assigned to each interface on the device.

Type

The type of the interface, distinguished by the physical/link protocol(s) running immediately below the network layer. Possible values are **sdlc** (for the backplane SMB 1 management interface), **Other** (for the 9H42x-xx module's two internal

Host interfaces and the backplane INB interface), and **ethernet-csmacd** (for both standard and Fast Ethernet front panel interfaces, and the backplane SMB 10 management interface).

Description

A text description of the interface: **SMB 1** and **SMB 10** (for the MMAC-Plus backplane management interfaces); **Host** (for the module's two internal host interfaces); **INB** (for the INB backplane interface), and **Ethernet** (for both standard and Fast Ethernet front panel interfaces).

P. Sta

Displays the current physical status — or operational state — of the interface: **Online** or **Offline**.

L. Sta

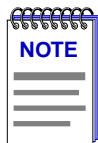
Displays the current logical status — or administrative state — of the interface: **Up** or **Down**.

Interface Performance Statistics/Bar Graphs

The statistical values and accompanying bar graphs to the right of the interface description fields provide a quick summary of interface performance. You can select the statistical value you want to display and the units in which you want those values displayed by using the two menu buttons directly above the graphs, as follows:

1. Click on the right menu button to select the unit in which you wish to display the selected statistic: , , or .
2. Once you have selected the base units, click on the left menu button to specify the statistic you'd like to display. (The options from this menu will vary depending on the base units you have selected.)

After you select a new display mode, the statistics and graphs will refresh to reflect the current choice, as described below.



*Bar graphs are only available when **Load** is the selected base unit.*

Raw Counts

The total count of network traffic received or transmitted on the indicated interface since device counters were last reset. Raw counts are provided for the following parameters:

In Octets	Octets received on the interface, including framing characters.
-----------	---

In Packets	Packets (both unicast and non-unicast) received by the device interface and delivered to a higher-layer protocol.
In Errors	Packets received by the device interface that contained errors that prevented them from being delivered to a higher-layer protocol.
In Discards	Packets received by the device interface that were discarded even though no errors prevented them from being delivered to a higher layer protocol (e.g., to free up buffer space in the device).
In Unknown	Packets received by the device interface that were discarded because of an unknown or unsupported protocol.
Out Octets	Octets transmitted by the interface, including framing characters.
Out Packets	Packets transmitted, at the request of a higher level protocol, by the device interface to a subnetwork address (both unicast and non-unicast).
Out Errors	Outbound packets that could not be transmitted by the device interface because they contained errors.
Out Discards	Outbound packets that were discarded by the device interface even though no errors were detected that would prevent them from being transmitted. A possible reason for discard would be to free up buffer space in the device.

Load

The number of bytes processed by the indicated interface during the last poll interval in comparison to the theoretical maximum load for that interface type (10 Mbps for standard Ethernet; 100 Mbps for Fast Ethernet). Load is further defined by the following parameters:

In Octets	The number of bytes received by this interface, expressed as a percentage of the theoretical maximum load.
Out Octets	The number of bytes transmitted by this interface, expressed as a percentage of the theoretical maximum load.

Rate

The count for the selected statistic during the last poll interval. The available parameters are the same as those provided for Raw Counts. Refer to the Raw Counts section, above, for a complete description of each parameter.

Viewing Interface Detail

The Interface Statistics window (Figure 2-6) provides detailed MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for each individual port interface. Color-coded pie charts also let you graphically view statistics for both received and transmitted Unicast, Multicast, Discarded, and Error packets.

To open the Interface Statistics window:

1. In the I/F Summary window, click to select the interface for which you'd like to view more detailed statistics.
2. Click on **Detail**. The appropriate I/F Statistics window, Figure 2-6, will appear.

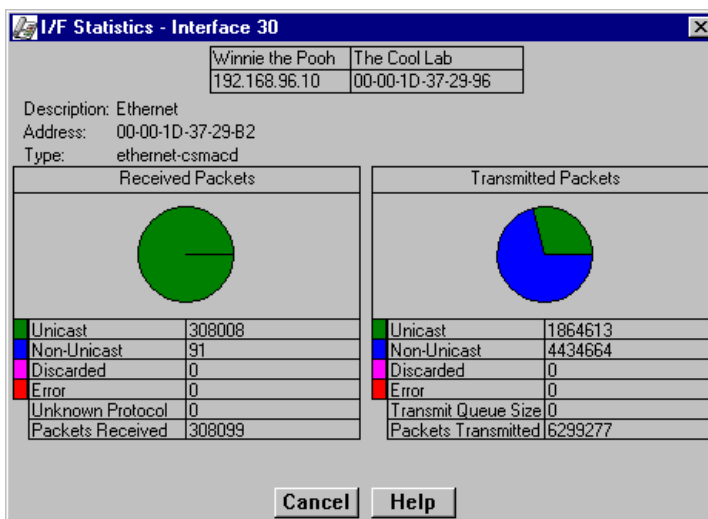
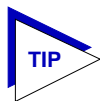


Figure 2-6. Detail Interface Statistics



You can also access this information via the I/F Statistics option available on the individual port menus; see Chapter 4, **Statistics**, for more information.

Three informational fields appear in the upper portion of the window:

Description

Displays the interface description for the currently selected interface: Ethernet, Host, SMB 1, SMB 10, or INB.

Address

Displays the MAC (physical) address of the selected interface.

Type

Displays the interface type of the selected port: ethernet-csmacd, sdlc, or other.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast

Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast

Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The multicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded

Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges or switches. Consult the Cabletron Systems *Network Troubleshooting Guide* for more information.

These statistics are displayed in the pie chart, color-coded magenta.

Error

Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol (Received only)

Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received (Received only)

Displays the number of packets received by the selected interface.

Transmit Queue Size (Transmit only)

Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the 9H42x-xx module will begin to discard packets.

Packets Transmitted (Transmit only)

Displays the number of packets transmitted by this interface.

Making Sense of Detail Statistics

The statistics available in this window can give you an idea of how an interface is performing; by using the statistics in a few simple calculations, it's also possible to get a sense of an interface's activity level:

To calculate the percentage of input errors:

Received Errors /Packets Received

To calculate the percentage of output errors:

Transmitted Errors /Packets Transmitted

To calculate the total number of inbound and outbound discards:

Received Discards + Transmitted Discards

To calculate the percentage of inbound packets that were discarded:

Received Discards /Packets Received

To calculate the percentage of outbound packets that were discarded:

Transmit Discards /Packets Transmitted

Using the Find Source Address Feature

You can use the Find Source Address option to discover the bridging interface through which a specific MAC address is communicating with the 9H42x-xx SmartSwitch. When you select **Find Source Address** from the Device menu, the device's Filtering Database is searched for an entry which designates the bridge interface serving as the source port for packets from the selected MAC address. If the search is successful, the associated port will flash on the Chassis View display; if the search is unsuccessful, a window will appear indicating that fact.

To search for a source address:

1. Click on **Device** in the Module View window to display the Device menu.
2. Drag down to **Find Source Address...**, and release. The Find Source Address window, [Figure 2-7](#), will appear.

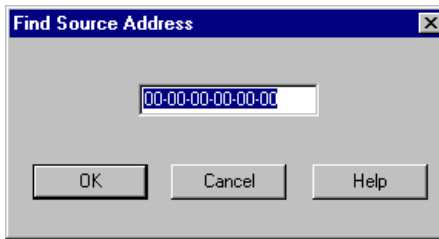


Figure 2-7. Find Source Address Window

3. In the text field, enter a valid MAC address in hexadecimal format, then click **OK**. If you enter an invalid address — that is, one not in hexadecimal xx-xx-xx-xx-xx-xx- format — an error window will appear indicating that the selected address is invalid.

If the selected MAC address is found in the 9H42x-xx module's Filtering Database, the bridge interface through which the address is communicating will flash in the Module View display.

If the address is not found, a window will appear indicating that the address could not be found.

Managing the Module

In addition to the performance and configuration information described in the preceding sections, the Module View also provides you with the tools you need to configure your module and keep it operating properly. Module management functions include configuring ports, setting the module date and time, and enabling and disabling ports.

Configuring Ports

The Configuration options available for standard Ethernet and Fast Ethernet ports allow you to configure operating parameters specific to each port type: for standard Ethernet ports, you can set the Duplex Mode; for Fast Ethernet ports, you can set a variety of duplex mode and negotiation parameters. Both standard Ethernet and Fast Ethernet Port Configuration windows are available from the Module View Port menus and from the Bridge Status window Port menus. There is no Configuration option available for the backplane INB interface.

Configuring Standard Ethernet Ports

The Port Configuration window available for standard Ethernet ports allows you to set an interface to either Standard or Full Duplex Mode. Full Duplex mode effectively doubles the available wire speed by allowing the interface to both receive and transmit simultaneously. This window will also display the mode currently in effect on the selected interface.

To access the Port Configuration Window:

1. From the Module View, click to select the port you wish to configure; the port menu will display;

or

From the Bridge Status window, click to select the port you wish to configure; the bridge port menu will display.

2. Drag down to **Configuration**, and release. The Port Configuration window, [Figure 2-8](#), will appear.

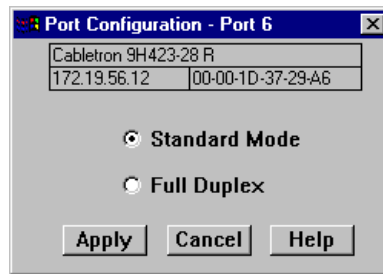
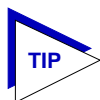


Figure 2-8. Port Configuration



Note that, if you select the Configuration option available for a Fast Ethernet interface, an entirely different window will appear; see [Configuring Fast Ethernet Ports](#), below, for information on configuring these ports.

Use the options in this window to select the desired mode:

Standard Mode

In Standard Mode, an interface can only either transmit *or* receive at any given time, and must wait for one activity to be completed before switching to the next activity (receive or transmit). In this mode, standard wire speeds (10 Mbps for Ethernet) are available.

Full Duplex

In Full Duplex Mode, an interface can both receive *and* transmit packets at the same time, effectively doubling the available wire speed to 20 Mbps.

Be sure to click on **Apply** to set your changes; note that the interface's current mode can be determined by the field selected in the window.

Configuring Fast Ethernet Ports

For any Fast Ethernet interface, the Port Configuration window allows you to both view and set that port's available modes. All 100Base-TX Fast Ethernet ports can be configured to operate in either standard Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) mode, and in each mode can be configured to operate in Full Duplex, effectively doubling the available wire speed (from 10 to 20 Mbps in standard Ethernet mode, or from 100 to 200 Mbps in Fast Ethernet mode); 100Base-FX (fiber) ports can be configured to operate in their standard 100 Mbps mode, or in full duplex mode. This window also displays the mode currently in effect on the selected interface, and provides some information (where it is available) about the interface's link partner.

To access the Port Configuration Window:

1. From the Module View, click to select the port you wish to configure; the port menu will display;

or

From the Bridge Status window, click to select the port you wish to configure; the bridge port menu will display.

2. Drag down to **Configuration**, and release. The Fast Ethernet Port Configuration window, [Figure 2-9](#), will appear.

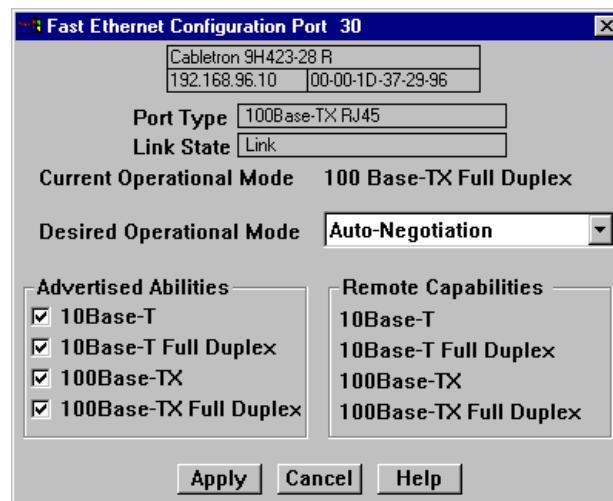
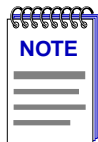
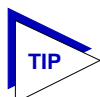


Figure 2-9. Fast Ethernet Configuration



The *Advertised Abilities* functionality is not supported by the FE-100FX Fast Ethernet port module; if you launch the Configuration window for one of these modules, the **Advertised Abilities** and **Remote Capabilities** sections of the window will be grayed out. If you launch the window for a port module slot which has no FE module installed, the Port Type will display as *Unknown*, the Link State will display *No Link*, and the rest of the fields will be blank and/or grayed out.



Note that, if you select the Configuration option available for a standard Ethernet interface, an entirely different window will appear; see **Configuring Standard Ethernet Ports**, page 2-20, for information on configuring these ports.

From this window you can manually set the operational mode of the port, or — for 100Base-TX interfaces — set the port to auto negotiation so that the appropriate operational mode can be determined automatically. The mode you set will determine the speed of the port and whether it uses Full Duplex or Standard Mode bridging.

The following information about the selected Fast Ethernet port is displayed:

Port Type

Displays the port’s type: 100Base-TX (for copper Fast Ethernet ports), 100Base-FX (for fiber Fast Ethernet ports), or Unknown (for a port slot with no module installed).

Link State

Displays the current connection status of the selected port: Link or No Link.

Current Operational Mode

Indicates which of the available operational modes is currently in effect: 10Base-T, 10Base-T Full Duplex, 100Base-TX, 100Base-TX Full Duplex, 100Base-FX, or 100Base-FX Full Duplex. If the port is still initializing, not linked, or if there is no port module installed in the slot, this field will remain blank.

Desired Operational Mode

Displays the operational mode that you have selected for this port, and allows you to change that selection. The following operational modes are available for each port:

- 100Base-TX** Auto Negotiation, 10Base-T, 10BASE-T Full Duplex, 100Base-TX, and 100Base-TX Full Duplex.
- 100Base-FX** 100Base-FX and 100Base-FX Full Duplex



If you choose to select a specific mode of operation (rather than auto-negotiation), you should be sure that the link partner supports the same mode. Otherwise, no link will be achieved.

If you select a Full Duplex mode and the link partner supports the same wire speed but not Full Duplex, a link will be achieved, but it will be unstable and will behave erratically.

If you select Auto-Negotiation, the local node will try to match the mode of the link partner, even if the link partner is not set to auto-negotiate, and even if the local node must use a mode which is it is not currently advertising.

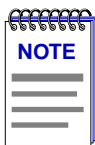
Note that if Auto Negotiation is the selected mode, the **Current Operational Mode** field will indicate which mode was selected by the link partners.

See **Setting the Desired Operational Mode**, [page 2-24](#), for more information.

Advertised Abilities

For 100Base-TX ports which have been configured to operate in Auto Negotiation mode, this field allows you to select which of the operational modes available to the port can be selected by the negotiating link partners. During Auto Negotiation, each of the link partners will advertise all selected modes in descending bandwidth order: 100Base-TX Full Duplex, 100Base-TX, 10Base-T Full Duplex, and 10Base-T. Of the selected abilities, the highest mode mutually available will automatically be used. If there is no mode mutually advertised, no link will be achieved.

If you have selected a specific operational mode for your 100Base-TX port, the Advertised Abilities do not apply; the selected Advertised Abilities also do not restrict the local node's ability to set up a link with a partner who is not currently Auto-Negotiating.



Auto-Negotiation is not currently supported for 100Base-FX ports; for these ports, the Advertised Abilities section will be grayed out.

Remote Capabilities

When the local node is set to Auto-Negotiation, this field will display the advertised abilities of the remote link — even if the remote link is not currently set to auto-negotiate. Possible values for this field are:

- 100Base-TX Full Duplex
- 100Base-TX
- 10Base-T Full Duplex
- 10Base-T

- Link Partner does not support auto negotiation — auto negotiation is either not supported by or is not currently selected on the remote port.
- Unknown — the link partner’s capabilities could not be determined.

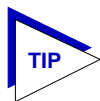
When the local node is *not* set to Auto-Negotiation, this field will be grayed out, even if the link partner is set to Auto-Negotiation and is advertising abilities.



If both link partners are set to Auto-Negotiation, but there is no mutually-advertised operational mode, no link will be achieved, and both nodes may display the message “Link Partner does not support Auto-Negotiation.” To resolve this situation, be sure both link partners advertise all their abilities, or be sure they advertise at least one mutually-available mode.

Setting the Desired Operational Mode

For any 100Base-TX port, you can specifically choose any one of the four available operational modes, or you can select Auto-Negotiation mode, which allows the port to negotiate with its link partner to find the highest mutually available bandwidth. If you select Auto Negotiation mode, you must also choose which of the port’s bandwidth capabilities you wish to advertise to the link partner.



If you select Auto-Negotiation at both ends of a link, be sure at least one mutually-advertised operational mode is available.

For a 100Base-FX port, the selection process is somewhat simpler; Auto Negotiation for these ports is not supported at this time, so you need only choose between 100Base-FX standard mode and 100Base-FX Full Duplex. However, you must still be sure that both link partners are set to the same operational mode, or the link will be unstable.

To set your desired operational mode:

1. Click in the **Desired Operational Mode** field to display the menu of available options; drag down to select the operational mode you wish to set.

For 100Base-TX ports, the available options are:

10Base-T — 10 Mbps connection, Standard Mode

10Base-T Full Duplex — 10 Mbps connection, Duplex Mode

100Base-TX — 100 Mbps connection, Standard Mode

100Base-TX Full Duplex — 100 Mbps connection, Duplex Mode

Auto Negotiation — the operational mode will be dynamically set based on the modes selected in the Advertised Abilities field (where both link partners are auto-negotiating) and the speeds and modes supported by the attached device

For 100Base-FX ports, options are:

100Base-FX — 100 Mbps connection, Standard Mode

100Base-FX Full Duplex — 100 Mbps connection, Duplex Mode

2. If you have selected Auto Negotiation (for 100Base-TX ports only), use the **Advertised Abilities** field to select the operational capabilities you wish to advertise to the port's link partner. If both link partners will be auto-negotiating, be sure there is at least one mutually-advertised operational mode, or no link will be achieved.



The selected Advertised Abilities only come into play when both link partners are auto-negotiating; if only one link partner is set to auto-negotiate, that node will establish a link at whatever mode its partner is set to, even if that mode is not currently being advertised.

3. Click on **Apply** to save your changes. Some window fields will refresh immediately and display the new settings; to manually refresh the window, simply close, then re-open it, or just re-select the **Configuration** option from the appropriate Port menu. Note that it may take a few minutes for mode changes to be completely initialized, particularly if the link partners must negotiate or re-negotiate the mode; you may need to refresh the window a few times before current operational data is displayed.

Setting the Device Date and Time

You can select the **Edit Device Time** and **Edit Device Date** options from the Device menu to change the date and time stored in the device's internal clock.

To edit the device time:

1. Click on **Device** on the Module View window menu bar to access the Device menu, drag down to **Edit Device Time...**, and release. The following change window, [Figure 2-10](#), will appear.

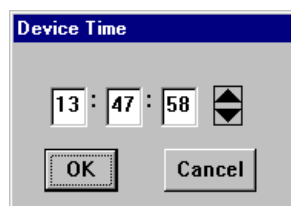


Figure 2-10. Edit Time Window

2. Enter the new time in a 24-hour hh:mm:ss format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by simply entering the new value in the appropriate field.
3. Click on **OK** to save the changes, or on **Cancel** to exit without changes.

To edit the device date:

1. Click on **Device** on the Module View window menu bar to access the Device menu, drag down to **Edit Device Date...**, and release. The following change window, [Figure 2-11](#), will appear.

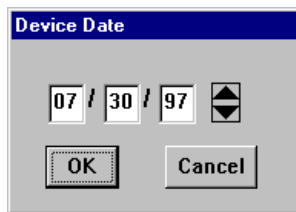


Figure 2-11. Edit Date Window

2. Enter the new date in a mm/dd/yy format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by simply entering the new value in the appropriate field.
3. Click on **OK** to save the changes, or on **Cancel** to exit without changes.

Enabling and Disabling Ports

When you disable bridging at a port interface, you disconnect that port's network from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge or with other networks connected to the bridge. When you enable bridging for the interface, the port moves from the Disabled state through the Listening and Learning states to the Forwarding state; bridge port state color codes will change accordingly.



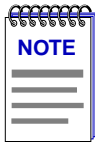
Before disabling bridging for any port, be sure that doing so will not sever your network connection.

To enable or disable bridging for an individual interface:

1. Click on the appropriate port display box to display the port menu.
2. Drag down to select **Enable** to enable bridging at the interface, or **Disable** to disable bridging. Bridging will now be enabled or disabled across the selected port, as desired.

To enable or disable bridging for all interfaces on the selected module:

1. Click on the **Bridge** label to display the Bridge menu.
2. Drag down to select **Enable Bridge** to enable bridging at all interfaces, or **Disable Bridge** to disable bridging across all interfaces. Bridging will now be enabled or disabled across the installed interfaces, as desired.



*For more information about bridging functions and how to determine the current state of each bridge port, see Chapter 5, **Bridging**.*

Alarm Configuration

Accessing the Basic and Advanced Alarms windows; creating a basic alarm; creating an advanced alarm; creating events; assigning actions to events; viewing the event log

Through the RMON Alarm and Event functionality supported by your 9H42x-xx, you can configure alarms and events (and, where appropriate, actions) for each available bridging interface.



*The Alarm, Event, and Actions windows described in this chapter are identical to those provided via the RMON utility. For more information about other features of RMON, see the **RMON User's Guide** included with your software.*

About RMON Alarms and Events

Although Alarms and Events are defined as separate RMON groups, neither one can function properly without the other: you can define an alarm threshold, but if it doesn't point to an event, there will be no indication that the threshold has been crossed; similarly, you can define an event, but unless it is attached to an alarm threshold, it won't be triggered. Each is an essential part of the same notification process: the alarm defines a set of conditions you want to know about, and the event determines the means of letting you know those conditions have occurred.

Events are also an integral part of the filter and packet capture functionality: you can start and stop packet capturing in response to events, or a successful packet capture can generate its own event.

SPECTRUM Element Manager provides two means for configuring RMON alarms: using the Basic Alarms window, you can define both rising and falling alarm thresholds for up to three pre-selected MIB-II variables per interface; based on the options you select, the application automatically creates the necessary events (to log alarm occurrences, generate a trap, or both) and — for Cabletron devices which support the new Actions MIB — adds the requested actions to those events (to enable or disable bridging at the selected interface).

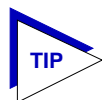
Using the Advanced Alarms feature, you can define custom alarms for almost any MIB-II or RMON object, as long as it is present in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). All aspects of these alarms are user-selectable: thresholds can be established on either the absolute or delta value for a variable; events can be configured to create a log, generate a trap, or both; and for Cabletron devices that support the new Actions MIB, events can also be configured to perform any defined SNMP SET or series of SETs on device objects. The Advanced Alarms feature also allows you to configure any events you wish to use in conjunction with the Packet Capture functionality. (For more information on using the Packet Capture feature, see the *RMON User's Guide* included with your software.)

The Basic Alarms feature allows you to assign alarms to any interface type; using the Advanced Alarms feature, you need only be sure to select variables appropriate to the interface — Ethernet for Ethernet, Token Ring for Token Ring, etc. — when defining your alarms.

Basic Alarm Configuration

Using the Basic Alarm Configuration application, you can define both rising and falling alarm thresholds for three selected MIB-II objects: ifInOctets, ifInNUcast, and ifInErrors. Because these pre-selected objects are not RMON-specific, you can configure alarms for all interfaces installed in your MMAC-Plus chassis — including those, like FDDI, for which no specific RMON statistics currently exist.

In addition to configuring separate rising and falling thresholds, you can also configure your device's *response* to an alarm condition: when a threshold is crossed, the RMON device can create a log of alarm events, send a trap notifying your management workstation that an alarm condition has occurred, or both; you can even configure an alarm to enable or disable bridging on the offending port in response to a rising or falling alarm condition.



*If you are familiar with the RMON MIB and/or with the original Alarm and Event functionality provided by SPECTRUM Element Manager (now known as the Advanced Alarm functionality), you will note that the Basic Alarm Configuration window combines the three parts of creating a working alarm — configuring the alarm itself, configuring an event that will announce the occurrence of an alarm (including assigning any actions), and linking the two — into a single step, and handles the details transparently. For more information about the individual steps involved in creating an alarm, see **Advanced Alarm Configuration**, page 3-11.*

Accessing the Basic Alarm Configuration Window

To access the RMON Basic Alarm Configuration window:

1. From the Module View, click on the appropriate port interface to display the Port menu.
2. Drag down to **Alarm Configuration**, and release. The RMON Basic Alarm Configuration window, [Figure 3-1](#), will appear.

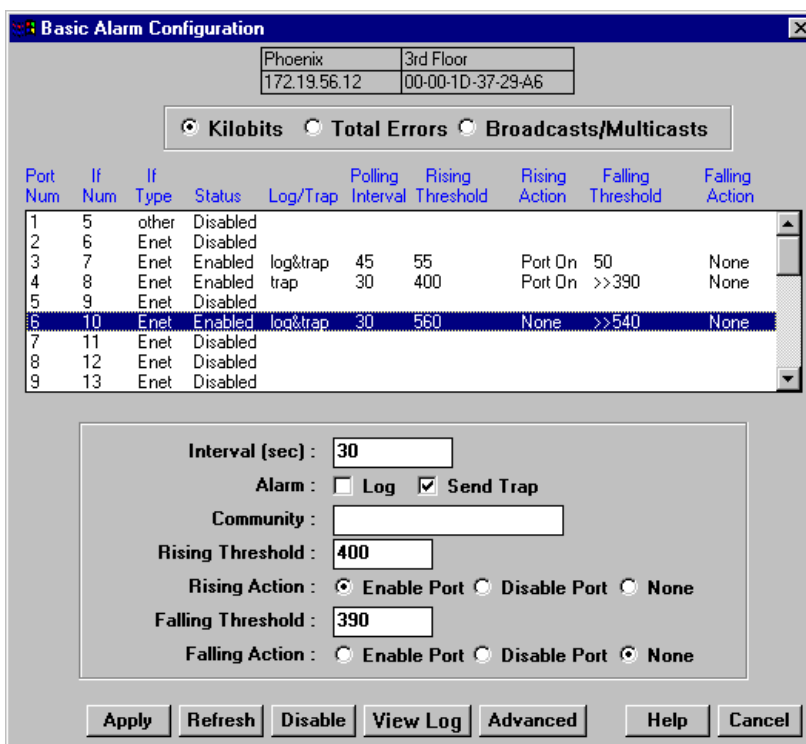
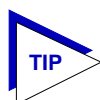


Figure 3-1. RMON Basic Alarm Configuration Window



You can also access the Alarms function — and the rest of the RMON functionality — by selecting the **RMON** option from the Module View Utilities menu.

When the window is first launched, no interfaces will be selected, and the **Apply**, **Disable**, and **View Log** buttons will be grayed out: **Apply** and **Disable** will activate when an interface is selected; **View Log** will activate when an interface which has experienced an alarm event is selected. The presence of an event log is indicated by the double greater-than sign (>>) displayed to the left of the threshold value that was crossed.

Viewing Alarm Status

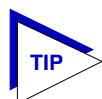
The Basic Alarm Configuration window contains all the fields you need to configure one or more of the three basic alarms available for each interface installed in your RMON device:

Kilobits — Total Errors — Broadcasts/Multicasts

Use these fields at the top of the window to change the alarm type whose status is displayed in the list box. For example, if the **Kilobits** option is selected, the information in the list box pertains to the status of the Kilobits alarm type for each installed interface. Before you configure an alarm or alarms, be sure the appropriate option is selected here.

The available alarm variables are:

- **Kilobits** (*ifInOctets*) — tracks the number of octets of data received by the selected interface. Note that this value has been converted for you from octets (or bytes) to kilobits (or units of 125 bytes); be sure to enter your thresholds accordingly. For example, to set a rising threshold of 1250 octets, enter a threshold value of 10; to set a falling threshold of 625 octets, enter a threshold value of 5.
- **Total Errors** (*ifInErrors*) — tracks the number of error packets received by the selected interface.
- **Broadcast/Multicast** (*ifInNUcast*) — tracks the number of non-unicast — that is, broadcast or multicast — packets received by the selected interface.



Note that the three pre-selected alarm variables are all MIB II variables; this allows you to configure alarms for any installed interface — even those for which no specific RMON statistics yet exist.

Port Number

Provides a sequential indexing of the interfaces installed in your RMON device.

IF Number

Displays the interface number assigned to each available interface. Note that because of the mismatch between physical interfaces on the device and the sequential port numbers assigned to the INB and the Ethernet/Fast Ethernet interfaces, the INB interface is indexed 5 and the Ethernet/Fast Ethernet interfaces are indexed 6 through 17.

IF Type

Displays each interface's type: Ethernet or Other (for the INB interface). Note that there is no type distinction between standard Ethernet and Fast Ethernet.

Status

Displays the current status of the selected alarm type for each interface: Enabled or Disabled. Remember, this status refers only to the alarm type which is selected at the top of the window; each of the other two alarm types can have different states.

Log/Trap

Indicates whether or not each alarm has been configured to create a silent log of event occurrences and the alarms that triggered them, and whether or not each alarm has been configured to issue a trap in response to a rising or falling alarm condition. Possible values are **log**, **trap**, **log&trap**, or **none**.

Polling Interval

Displays the amount of time, in seconds, over which the selected alarm variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds (described below). You can set any interval from 1 to 65,535 seconds.

Rising Threshold

Displays the high threshold value set for the selected alarm variable. Values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Rising Action

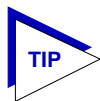
Indicates whether or not a rising alarm occurrence will initiate any actions in response to the alarm condition: **Enable** if bridging will be enabled at the selected interface in response to a rising alarm, **Disable** if bridging will be disabled at the selected interface in response to a rising alarm, and **None** if no actions have been configured for the selected alarm. Note that the Action fields will be unavailable for devices configured to operate in SecureFast switching mode.

Falling Threshold

Displays the low threshold value set for the selected alarm variable. Values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Falling Action

Indicates whether or not a falling alarm occurrence will initiate any actions in response to the alarm condition: **Enable** if bridging will be enabled at the selected interface in response to a falling alarm, **Disable** if bridging will be disabled in response to a falling alarm, and **None** if no actions have been configured for the selected alarm. Note that the Action fields will be unavailable for devices configured to operate in SecureFast switching mode.



Before you decided whether or not to assign an action to a rising or falling alarm, it is important to understand something about the hysteresis function built in to the RMON alarm functionality. See [How Rising and Falling Thresholds Work](#), page 3-27, for more information.

The remainder of the window fields provide the means for configuring alarms for each available interface. Note that the information provided in this screen is static once it is displayed; for updated information, click on **Refresh**. Adding or modifying an alarm automatically updates the list.

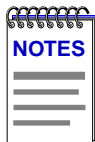
Creating and Editing a Basic Alarm

The editable fields at the bottom of the Basic Alarm Configuration window allow you to configure alarm parameters for each available interface. These fields will display the parameters used for the most recently configured alarm (no matter which interfaces are selected in the list box); this allows you to set the same parameters on multiple interfaces with a single set. Hold down the **Shift** key while clicking to select a contiguous group of interfaces; use the **Ctrl** key to select any interfaces. To display the alarm parameters for a specific interface, double-click on that interface.

Note that there is no specific “Enable” function; simply configuring thresholds and/or actions for an alarm and applying those changes enables the alarm. For more information on disabling an alarm, see [Disabling a Basic Alarm](#), page 3-9.

To configure an alarm:

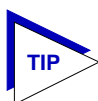
1. At the top of the window, click to select the variable to be used for your alarm: **Kilobits**, **Total Errors**, or **Broadcast/Multicast**. The display in the list box will reflect the current status at each interface of the alarm type you have selected.
2. In the list box, click to highlight the interface (or use **shift-click** or **ctrl-click** to select multiple interfaces) for which you would like to configure an alarm for the selected variable. Note that the editable fields will display the parameters assigned to the most recently set alarm; however, any changes you make in these fields will be set to all selected interfaces.
3. In the **Interval** field, enter the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. You can assign any interval from 1 to 65,535.
4. In the **Alarm** field, click to select one or both of the following options:
 - a. Select **Log** if you wish to create a silent log of alarm occurrences.
 - b. Select **Trap** if you want your device to issue a trap in response to each alarm occurrence.



In order for the trap selection to work properly, your 9H42x-xx must be configured to send traps to your network management station. This can be accomplished via the Remote Administration Tools application or via Local Management and the Trap Table. See the **Remote Administration Tools User's Guide** and/or your device hardware manual for more information.

*If you are monitoring a variable you consider to be critical, we do not recommend that you select **Trap** as the only event response; if a trap is lost due to a collision or other transmission problem, it will not be re-sent.*

5. Any value you enter in the **Community** field will be included in any trap messages issued by your 9H42x-xx in response to the alarm(s) you are configuring; this value is also used to direct traps related to this alarm to the appropriate management workstation(s):
 - a. **If you enter a value in this field**, traps related to the associated alarms will only be sent to the network management stations in the device's trap table which have been assigned the same community name (and for which traps have been enabled). Any IP addresses in the device's trap table which have not been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.
 - b. **If you leave this field blank**, traps related to the associated alarms will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled — regardless of whether or not those IP addresses have been assigned a community name in the Trap Table.



For more information about configuring the 9H42x-xx's Trap Table, consult the **Remote Administration Tools User's Guide** and/or your Local Management documentation. (Remember, no traps will be sent by your 9H42x-xx at all unless its Trap Table has been properly configured!)

6. Click in the **Rising Threshold** field; enter the high threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Remember, too, when configuring a **Kilobits** alarm, SPECTRUM Element Manager converts octets into kilobits (units of 125 bytes, or octets) for you; for example, to set a rising threshold of 1250 octets, enter a threshold value of 10.

7. In the **Rising Action** field, click to select the action you want your device to take in response to a rising alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only bridging at the specified port, and not the interface itself.

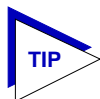
For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, [page 3-27](#).

8. Click in the **Falling Threshold** field; enter the low threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Remember, too, when configuring a **Kilobits** alarm, SPECTRUM Element Manager converts octets into kilobits (units of 125 bytes, or octets) for you; for example, to set a falling threshold of 625 octets, enter a threshold value of 5.

9. In the **Falling Action** field, click to select the action you want your device to take in response to a falling alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only bridging at the specified port, and not the interface itself.

For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, [page 3-27](#).



Remember, the Actions fields will be grayed out for devices configured to operate in SecureFast switching mode, as there is no active bridging component on those interfaces.

10. Click to set your changes. If you have made any errors in configuring alarm parameters (using an invalid rising or falling threshold, for example, or neglecting to supply a polling interval), either an error window with the appropriate message will appear, or a beep will sound and the cursor will blink in the field which contains the error. Correct the noted problem(s), and click again.

Once you click , the configured alarm parameters will be set for every selected interface, and the alarms will automatically be enabled; the list box display will also refresh to reflect these changes.

To configure additional alarms, or alarms of a different type, select the appropriate alarm variable at the top of the window, highlight the appropriate interface(s), and repeat the procedures outlined above.

Disabling a Basic Alarm

Using the **Disable** button at the bottom of the window actually performs two functions: it both disables the alarm and deletes the alarm entry (and its associated event and action entries) from device memory to help conserve device resources. In the list box display, the parameters for any “disabled” alarm are automatically reset to their default values.

To disable an alarm:

1. In the top of the window, click to select the variable for which you wish to disable an alarm: **Kilobits**, **Total Errors**, or **Broadcast/Multicast**.
2. In the list box display, click to highlight the interface(s) for which you wish to disable the selected alarm type. (Remember, you can use **shift-click** to select a sequential group of interfaces, or **ctrl-click** to select any group of interfaces.)
3. Click on **Disable**. The selected alarm type on the selected interface(s) will be disabled, and the list box display will refresh to reflect those changes.

Viewing the Basic Alarm Log

If you have selected the “log” response for an alarm, and that alarm’s rising and/or falling threshold has been crossed, the Basic Alarms application will create a log of alarm occurrences. If a threshold has been crossed, it will be preceded in the interface list box display by a double greater-than sign (>>). Clicking to select an interface which is so marked will activate the **View Log** button; selecting the **View Log** button will launch the appropriate Basic Alarm Log, [Figure 3-2](#). (Note that selecting more than one interface — even if all selected interfaces have experienced alarm conditions — will inactivate the **View Log** button; you can only view a single alarm log at a time.)

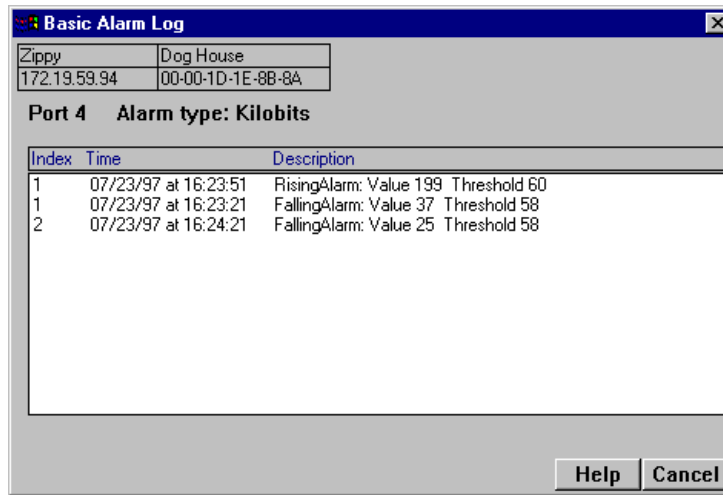
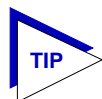


Figure 3-2. Basic Alarm Log

The top portion of the Basic Alarm Log window contains the device information boxes, as well as the Port Number assigned to the interface that experienced the alarm condition and the type of alarm that was triggered; the remainder of the window contains the following information about each alarm occurrence:

Index This index number uniquely identifies each *occurrence* of a rising or falling event. Note that, since the alarm whose log is displayed in [Figure 3-2](#) experienced both rising and falling alarms, there are two sets of event indices: one which identifies each instance of the rising alarm, and one which identifies each instance of the falling alarm.



For more information about the relationship between rising and falling alarms and the hysteresis function that controls the generation of alarm events, see [How Rising and Falling Thresholds Work](#), page 3-27.

Time Indicates the date and time of each event occurrence.

Description Provides a detailed description of the condition which triggered the alarm, including whether it was a Rising or Falling alarm, the Value which triggered the alarm, and the configured Threshold that was crossed.

Each log will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

Advanced Alarm Configuration

The Basic Alarm Configuration window provides a quick and easy way to set up some basic alarms for all of the interfaces installed in your 9H42x-xx. However, if you prefer more control over the parameters of the alarms you set (as well as their associated events and actions) and/or a wider array of choices for each variable, the Advanced Alarm feature provides a powerful and flexible means for configuring alarms, events, and actions to suit your particular networking needs.

Accessing the RMON Advanced Alarm/Event List

To access the RMON Advanced Alarm/Event List window:

1. In the Module View, click on the appropriate port interface to display the Port menu; drag down to **Alarm Configuration**, and release.
2. In the Basic Alarm Configuration window, click on **Advanced**; the RMON Advanced Alarm/Event List window, [Figure 3-3](#), will appear.

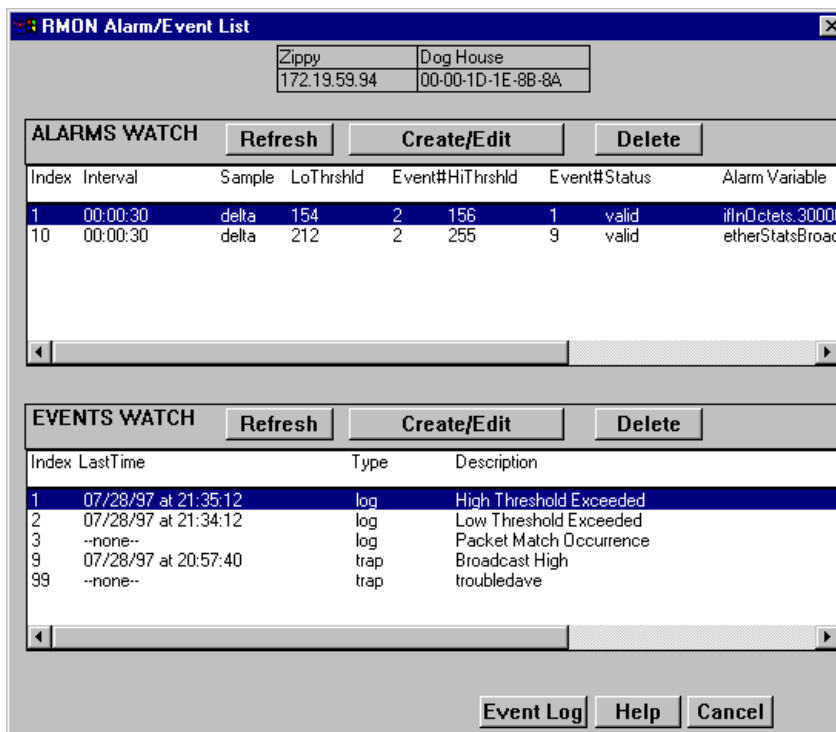
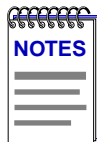


Figure 3-3. The RMON Advanced Alarm/Event List Window



Neither the Alarms or Events list is interface-specific; both will be displayed the same for every interface.

Note, too, that alarms and events which have been configured via the Basic Alarms window are not displayed in and cannot be accessed or edited from the Advanced Alarm/Event List window.

The top portion of the window displays the usual device information boxes; the remainder of the window contains the Alarms Watch and Events Watch lists, and the command buttons that allow you to create, edit, and delete entries in those lists, or refresh the display.

The fields in the Alarms Watch display include:

Index	The index is a number that uniquely identifies each alarm. Index numbers are user-defined; you can use any indexing scheme that works for you. These numbers are permanently assigned to their associated alarms; however, index numbers made available by the deletion of existing alarms can be assigned to new alarms, as needed. Note that indices 2000 to 3999 are reserved and unavailable.
Interval	Indicates the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value is compared to both the rising and falling thresholds configured for the alarm.
Sample	Indicates whether the sample value to be compared to the thresholds is an absolute , or total value — that is, the total value counted for the selected variable — or a relative, or delta value — the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval.
LoThrshld	Indicates the set value for the low, or falling threshold.
Event #	Indicates the event index number that the falling threshold points to: this is the event that will be triggered if the falling threshold is met or crossed. If the value for this field is zero, no event will be triggered.
HiThrshld	Indicates the set value for the high, or rising threshold.
Event #	Indicates the event index number that the rising threshold points to: the event that will be triggered if the rising threshold is met or crossed. If the value for this field is zero, no event will be triggered.
Status	Indicates the status of the alarm: valid, invalid, or underCreation. An alarm that is invalid is not functional; it may be referring to a MIB component that is inactive

(such as the Hosts component), not present, or unreachable, or it may have been deleted by software but not yet removed from memory at the device. An alarm that is underCreation is in the process of being configured (possibly by another management station), and should not be modified until its status is valid; if it never reaches valid status, it will eventually be removed.

Alarm Variable Indicates the variable that is being watched. You can use the scroll bar, if necessary, to view the complete name.

Note that the information provided in this screen is static once it is displayed; for updated information, click on **Refresh**. Adding or modifying an alarm automatically updates the list.

The fields in the Events Watch display include:

Index	This is a number that uniquely identifies an entry in the event table; an index number is assigned when an event is created. These numbers are extremely important, as they are the means by which an event is associated with an alarm or a packet capture filter. As with alarms, these index numbers are user-defined and can be assigned according to any indexing scheme that works for you. Index numbers are permanently assigned to their associated events; however, numbers made available by the deletion of existing events can be assigned to new events, as needed. Note that indices 2000 to 4999 are reserved and unavailable.
LastTime	Indicates the last time this event was triggered. Note that this information is static once it is displayed, and the LastTime field will not be updated unless you close, then open, the Alarms/Events window, or click on Refresh .
Type	Indicates the type of response that will be generated if the event is triggered: log, trap, or log & trap. A type of "none" indicates that occurrences of the event will not be logged and no trap will be sent; however, note that this field does not indicate whether or not there are any actions associated with the selected event.
Description	This is a user-defined text description used to identify the event and/or the alarm or packet capture that triggers it.

The **Event Log** button at the bottom of the screen provides access to the log which lists the occurrences of an event.

Note that the information provided in this screen is static once it is displayed; for updated information, click on **Refresh**. Adding or modifying an event automatically updates the list.

Creating and Editing an Advanced Alarm

The Create/Edit Alarms window (Figure 3-4) allows you to both create new alarms and edit existing ones. When you click on **Create/Edit** in the Alarms Watch list, the Create/Edit Alarms window will display the parameters of the alarm which is currently highlighted in the list. (If no alarms have yet been configured, a set of default parameters will be displayed.) All of these parameters are editable: to change an existing alarm, edit any parameter *except* the Index value; to create an entirely new alarm, simply assign a new Index number. The ability to assign index numbers allows you to quickly and easily create a number of similar alarms without having to close, then re-open the window or re-assign every parameter.

Note, too, that the main Alarm/Event window remains active while the Create/Edit Alarm window is open; to edit a different alarm (or use its settings as the basis of a new alarm), simply double-click on the alarm you want to use in the main Alarms Watch list, and the Create/Edit Alarm window will update accordingly.

To configure an alarm:

1. **If you wish to modify an existing alarm** or create a new alarm based on the parameters of an existing one, be sure the alarm of interest is highlighted in the Alarms Watch list, then click on **Create/Edit** at the top of the Alarms Watch portion of the RMON Advanced Alarm/Event List. The Create/Edit Alarms window, Figure 3-4, will appear.

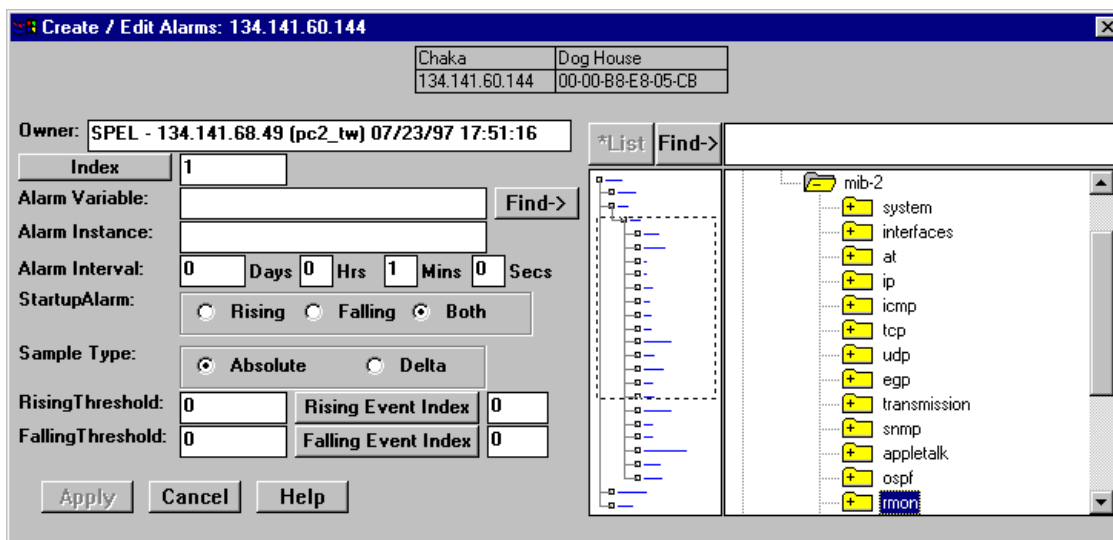
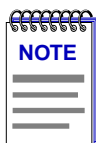



Figure 3-4. The RMON Create/Edit Alarms Window


If you wish to create an entirely new alarm, it doesn't matter which existing alarm (if any) is highlighted when you open the Create/Edit Alarms window; although the window will, by default, display the parameters of whichever alarm is currently selected, all parameters are editable and can be configured as desired.



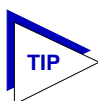
Whether you are modifying an existing alarm or creating a new one is determined solely by the assignment of the Index number: if you assign a previously unused index number, a new alarm instance will be created; if you use an existing index number, its associated alarm will be modified.

2. In the **Owner** text box, enter some appropriate text designation for this alarm, if desired; you may want to use the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the alarm. Since any workstation can access and change the alarms you are setting in your 9H42x-xx, some owner identification can prevent alarms from being altered or deleted accidentally. The default value provided is SPEL — <IP address> <(hostname)> <date> <time>, where <IP address> and <(hostname)> refer to the workstation that created the alarm and <date> and <time> reflect the date and time of the alarm's creation.
3. **If you are creating a new alarm**, use the **Index** field to assign a unique, currently unused index number to identify the alarm. Clicking on the  button will automatically assign the lowest available number; you can also click directly in the text box and assign any value you want between 1 and 1,999 and 4,000 and 9,999 (indices 2000 to 3999 are reserved and unavailable).



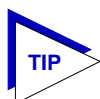
Clicking on  to select the next available index number will replace the current Owner string with the default value described above; if the default value is already in place, the date and time will be updated.

If you wish to modify an existing alarm, enter the appropriate index value, or double-click on the alarm of interest in the Alarms Watch list (in the main Alarm/Event window).



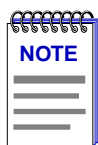
Remember, the only thing that determines whether you are modifying an existing alarm or creating a new one is the assignment of the index number; be sure to assign this value appropriately.

4. To select the **Variable** to be used for your alarm, use the MIBTree panel provided on the right side of the window. (For more information about how to use the MIBTree panel, see the **MIB Tools** chapter in the **Tools Guide**.) The display will default to the top of the tree (labeled Internet); there are three ways to locate and/or assign the correct variable:
 - a. If you know the exact name of the OID whose value you wish to track, simply enter the name in the **Alarm Variable** field; to verify that you have entered the name correctly, click on **Find->** to move the MIBTree display to that OID. (If the MIBTree display does not adjust to show the OID you've entered, you've entered the name incorrectly.)
 - b. Use the Radar View panel located just left of the MIB Tree panel to adjust the MIB Tree display to the part of the tree that contains the variable you are interested in, then click to open the appropriate folders. (Again, see the **Tools Guide** for more details on using the Radar View.)
 - c. Use the scroll bars and click to open the appropriate folders in the MIBTree panel to locate the object you wish you use; click to select it in the panel, and its name will automatically be entered in the **Alarm Variable** field.



*If you don't know the exact spelling of the OID you wish to use for your alarm variable, and you can't find it by searching through the tree, use the MIBTree utility's Find feature to locate the OID and determine its exact spelling (and tree location). For more information on the MIBTree panel and its Find capabilities, see Chapter 3, **MIB Tools**, in the **SPECTRUM Element Manager Tools Guide**. Note that this Find feature is no longer case-sensitive.*

Almost any RMON or MIB-II object can be used as an alarm variable as long as it is resident in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). If you select an invalid object (i.e., one whose value is not an integer), the message “!!Can't set alarm on this type!!” will display in the Alarm Variable field.



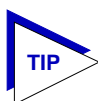
*If you select an object which is not resident in the device firmware, you will receive a “Set Failed; ensure variable is readable” message when you try to set your alarm by clicking on **Apply**. If you are unsure just which objects are resident on your device, and you find yourself receiving a lot of “Set Failed” messages, you can use the MIB Tools utility (accessed from the primary window menu bar or from the Module View) to determine which objects are and are not part of your device's firmware — simply query the object you are interested in; if the query response comes back empty, the object is not present (make sure you are using the appropriate community name when making a query, or you will get no response).*

5. Once you have selected the object you wish to use for your alarm variable, you must assign the appropriate instance value in the **Alarm Instance** field. Most RMON objects are instantiated by the index number assigned to the table in which they reside; for example, if you wish to set an alarm on an object

located in an RMON Statistics table, you can determine the appropriate instance by noting the index number assigned to the table that is collecting data on the interface you're interested in. In the case of the default tables, index numbers often mirror interface numbers; however, if there are multiple default tables per interface, or if additional tables have been created, this may not be true. (Table index numbers are assigned automatically as table entries are created; no two tables — even those on different interfaces — will share the same table index number.)

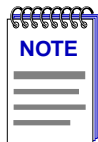
If you have selected an object from a table which is indexed by some other means — for example, by ring number — you must be sure to assign the instance accordingly. If you're not sure how a tabular object is instanced, you can use the MIBTree panel (described in the **Tools Guide**) to query the object; all available instances for the object will be displayed. (Host and matrix table objects — which are indexed by MAC address — require special handling; see the Note which follows this step.)

If you have selected an object which is not part of a table, you must assign an instance value of 0.



*You can use the MIBTree panel to determine which objects are tabular and which are not: objects which are part of a table will descend from a **blue** folder (which will have a "T" on it, and a name which will almost always include the word "table"); objects which are not will descend directly from a **yellow** folder. (**Note:** There may be one or more yellow folders in between the blue folder which contains the table and the leaf object you wish to use; however, those objects are still part of the table.)*

Be sure you define your instance values carefully; if you neglect to set the instance correctly, you will receive the "Set failed; ensure variable is readable" error message when you click to set your alarm.



If you wish to set an alarm on an object whose instance is non-integral — for example, a Host Table object indexed by MAC address — or on an object with multiple indices, like a Matrix Table entry (which is indexed by a pair of MAC addresses), you must follow certain special procedures for defining the instance. For these OIDs, the instance definition must take the following format:

table index.length(in bytes).instance(in decimal format)

For the first byte of the instance, you must use the index number of the **table** which contains the OID you want to track. For example, to set an alarm on an object in the Host Table, define the first byte of the instance as the index number assigned to the specific Host Table you want to check. These index numbers are assigned automatically as the table entries are created; no two tables — even if they are on different interfaces — will share the same table index number.

Second, you must specify the length, in bytes, of the index you will be using. Again, in the case of an object in the Host Table, that value would be 6, since Host Table entries are indexed by MAC address — a six-byte value.

Finally, you must specify the index itself, in **decimal** format. In the case of a MAC address, that means you must convert the standard hexadecimal format to decimal format. To do this, simply multiply the first digit of the two-digit hex number by 16, then add the value of the second digit. (For hex values represented by alphabetical characters, remember that a=10, b=11, c=12, d=13, e=14, and f=15.) A hex value of b7, for instance, is represented in decimal format as $16 \times 11 + 7$, or 183.

So, for example, the instance for an object in the Hosts group might read as follows:

2.6.0.0.29.170.35.201

where 2=the host table index; 6=the length in bytes of the index to follow; and 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9.

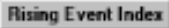
For objects with multiple indices — such as objects in a matrix table — you must add additional length and index information to the instance definition, as illustrated below:

3.6.0.0.29.170.35.201.6.0.0.29.10.20.183


where 3=the matrix table index; 6=the length in bytes of the index to follow; 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9; 6=the length in bytes of the next index; and 0.0.29.10.20.183=the decimal format for MAC address 00-00-1d-0a-14-b7.

Additional instance issues may exist for FDDI objects; if you're unsure how to assign an instance, use the MIB Tools utility to query the object of interest, and note the appropriate instancing on the returned values.

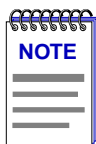
6. In the **Alarm Interval** field, enter the amount of time over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. There is no practical limit to the size of the interval (as the maximum value is 24,855 days 3 hours 14 minutes and 7 seconds — over 68 years!); the default value is 1 minute.

7. Since the first sample taken can be misleading, you can use the selections in the **Startup Alarm** box to disable either the rising or the falling threshold for that sample only. If you would like to exclude the falling alarm, select the **Rising** option; the first sample taken will only generate a rising alarm, even if the sample value is at or below the falling threshold. To exclude the rising alarm, select the **Falling** option; the first sample will then only generate a falling alarm, even if the sample value is at or above the rising threshold. If you wish to receive both alarms as appropriate, select the **Both** option.
8. Use the selections in the **Sample Type** box to indicate whether you want your threshold values compared to the total count for the variable (**Absolute**), or to the difference between the count at the end of the current interval and the count at the end of the previous interval (**Delta**). Make sure you have set your thresholds accordingly.
9. Click in the **RisingThreshold** field; enter the high threshold value for this alarm.
10. There are two ways to assign an event to your rising threshold: click in the **RisingEventIndex** text box and enter the number of the event you would like to see triggered if the rising threshold is crossed; or use the Events Watch list in the main Alarm/Event window to highlight the desired event, then click on . Be sure you assign the number of a valid event or there will be no response if the selected variable meets or crosses this threshold; assigning an index of zero effectively disables the threshold, as there will be no indication that it has been crossed.

For more information on how events are triggered, see **How Rising and Falling Thresholds Work**, [page 3-27](#).

11. Click in the **FallingThreshold** field; enter the low threshold value for this alarm.
12. There are two ways to assign an event to your falling threshold: click in the **FallingEventIndex** text box and enter the number of the event you would like to see triggered if the falling threshold is crossed; or use the Events Watch list in the main Alarm/Event window to highlight the desired event, then click on . Again, be sure you assign the number of a valid event or there will be no response if the selected variable meets or crosses this threshold; assigning an index of zero effectively disables the threshold, as there will be no indication that it has been crossed.

For more information on how events are triggered, see **How Rising and Falling Thresholds Work**, [page 3-27](#).



There is no limit to the number of alarms that may be assigned to the same event.

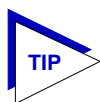
13. Click **Apply** to set your changes. If you have made any errors in configuring alarm parameters (using an invalid value in any field, leaving a field blank, or selecting an alarm variable which is not resident on the device), an error window with the appropriate message will appear. Correct the noted problem(s), and click **Apply** again.

Note that the window remains open so that you may configure additional new alarms or modify existing ones; remember, you can double-click on any alarm in the Alarms Watch list in the main Alarm/Event window to display its parameters in the Create/Edit Alarm window. When you have finished configuring your alarms, click on **Cancel** to close the window.

Creating and Editing an Event

The Create/Edit Events window (Figure 3-5, page 3-21) — like the Create/Edit Alarms window — allows you to both create new events and edit existing ones. When you click on the **Create/Edit** button in the Events Watch list, the Create/Edit Events window will display the parameters of the event which is currently highlighted in the list. (If no events have yet been configured, a set of default parameters will be displayed.) All of these parameters are editable: to change an existing event, edit any parameter *except* the Index value; to create an entirely new event, simply assign a new Index number. The ability to assign index numbers allows you to quickly and easily create a number of similar events without having to close, then re-open the window or re-assign every parameter.

Note, too, that the main Alarm/Event window remains active while the Create/Edit Event window is open; to edit a different event (or use its settings as the basis of a new event), simply double-click on the event you want to use in the main Events Watch list, and the Create/Edit Event window will update accordingly.



If the Create/Edit Actions window is also open, it too will update to display the actions associated with the event currently selected in the main Alarm/Event window. See [Adding Actions to an Event](#), page 3-23, for more information on the actions feature.

To configure an event:

1. **If you wish to modify an existing event** or create a new event based on the parameters of an existing one, be sure the event of interest is highlighted in the Events Watch list, then click on **Create/Edit** at the top of the Events Watch portion of the RMON Advanced Alarm/Event List. The Create/Edit Events window, Figure 3-5, will appear.

If you wish to create an entirely new event, it doesn't matter which existing event (if any) is highlighted when you open the Create/Edit Events window; although the window will, by default, display the parameters of whichever event is currently selected, all parameters are editable and can be configured as desired.

Name	Location
172.19.59.76	00-00-1D-0F-FD-B6

Index: 45

Description: Broadcast Storm Pending

Community:

Owner: SPEL - 134.141.68.49 (pc2_tw) 07/23/97 15:06:42

Event Type: Log Trap Actions

Apply Cancel Help

Figure 3-5. The RMON Create/Edit Events Window



Whether you are modifying an existing event or creating a new one is determined solely by the assignment of the Index number: if you assign a previously unused index number, a new event instance will be created; if you use an existing index number, its associated event will be modified.

2. **If you are creating a new event**, use the **Index** field to assign a unique, currently unused index number to identify the event. Clicking on the **Index** button will automatically assign the lowest available number; you can also click directly in the text box and assign any value you want between 1 and 1,999 and 5,000 and 9,999 (indices 2000 to 4999 are reserved and unavailable).



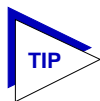
Clicking on **Index** to select the next available index number will replace the current Owner string with the default value; if the default value is already in place, the date and time will be updated.

If you wish to modify an existing event, enter the appropriate index value, or double-click on the event of interest in the Events Watch list (in the main Alarm/Event window).



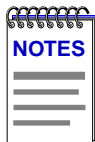
Remember, the only thing that determines whether you are modifying an existing event or creating a new one is the assignment of the index number; be sure to assign this value appropriately.

3. Click in the **Description** text box to enter any text description you want to identify the event. This description will appear in the Events Watch window and help you distinguish among the events you have configured.
4. Any value you enter in the **Community** field will be included in any trap messages issued by your 9H42x-xx when this event is triggered; this value is also used to direct traps related to this event to the appropriate management workstation(s):
 - a. **If you enter a value in this field**, traps related to this event will only be sent to the network management stations in the device's trap table which have been assigned the same community name (and for which traps have been enabled). Any IP addresses in the device's trap table which have not been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.
 - b. **If you leave this field blank**, traps related to this event will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled — regardless of whether or not those IP addresses have been assigned a community name in the Trap Table.



*For more information about configuring your 9H42x-xx's Trap Table, see the **Remote Administration Tools User's Guide** and/or your *Local Management* documentation. (Remember, no traps will be sent by your 9H42x-xx at all unless its Trap Table has been properly configured!)*

5. You can use the **Owner** text box for administrative or informational purposes; although the text entered here will not appear on any other screens, you may want to use the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the owner of the event. Since any workstation can access and change the events you are setting in your 9H42x-xx, some owner identification can prevent events from being altered or deleted accidentally. The default value provided is SPEL — <IP address> <(hostname)> <date> <time>, where <IP address> and <(hostname)> refer to the workstation that created the event and <date> and <time> reflect the date and time of the event's creation.
6. Use the options in the **Event Type** field to define how this event will respond when an associated threshold is crossed:
 - a. Select the **Log** option to create a silent log of event occurrences and the alarms that triggered them. Each event's log can be viewed by clicking on **Event Log** at the bottom of the Alarm/Event window. (See **Viewing an Advanced Alarm Event Log**, [page 3-26](#), for more information.)
 - b. Select **Trap** to instruct the device to send a pair of SNMP traps (one WARNING, one Normal) to the management station each time the event is triggered.

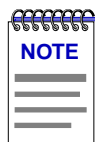


In order for the trap selection to work properly, your 9H42x-xx must be configured to send traps to the management station. This is accomplished via local management; consult your device hardware manual for more information.

If you are monitoring a variable you consider to be critical, we do not recommend that you select **Trap** as the only event response; if a trap is lost due to a collision or other transmission problem, it will not be re-sent.

- c. Select both **Log and Trap** to both log the event occurrence and generate the traps.

If you select neither option, the event's occurrences will neither be logged nor generate traps; unless the event includes an action or a series of actions, this effectively disables the event (since there will be no indication that it has been triggered).



The Event Type field in the Advanced Alarm/Event List window will display a value of "none" if neither the Log nor the Trap response has been selected; note, however, that this field does not indicate whether or not an event has been configured to perform an SNMP SET or series of SETs via the Actions MIB.

7. For Cabletron devices which support the proprietary Actions MIB, an **Actions** button will appear in the Create/Edit Events window; using this feature, you can configure an SNMP SET or series of SETs that will be performed automatically when the event is triggered. See **Adding Actions to an Event**, below, for more information.
8. Click **Apply** to set your changes. Note that the window remains open so that you may configure additional new events or modify existing ones; remember, you can double-click on any event in the Events Watch list in the main Alarm/Event window to display its parameters in the Create/Edit Event window (and in the Create/Edit Actions window, if it's open). When you have finished configuring your events, click on **Cancel** to close the window.

Adding Actions to an Event

For Cabletron devices which support the proprietary Actions MIB, selecting the **Actions** button in the Create/Edit Events window opens the Create/Edit Actions window (Figure 3-6), which allows you to define an SNMP SET or series of SETs that will be performed automatically when the associated event is triggered.

To add an action or series of actions to an event:

1. In the Create/Edit Events window, click on **Actions**. The Create/Edit Actions window, Figure 3-6, will appear.

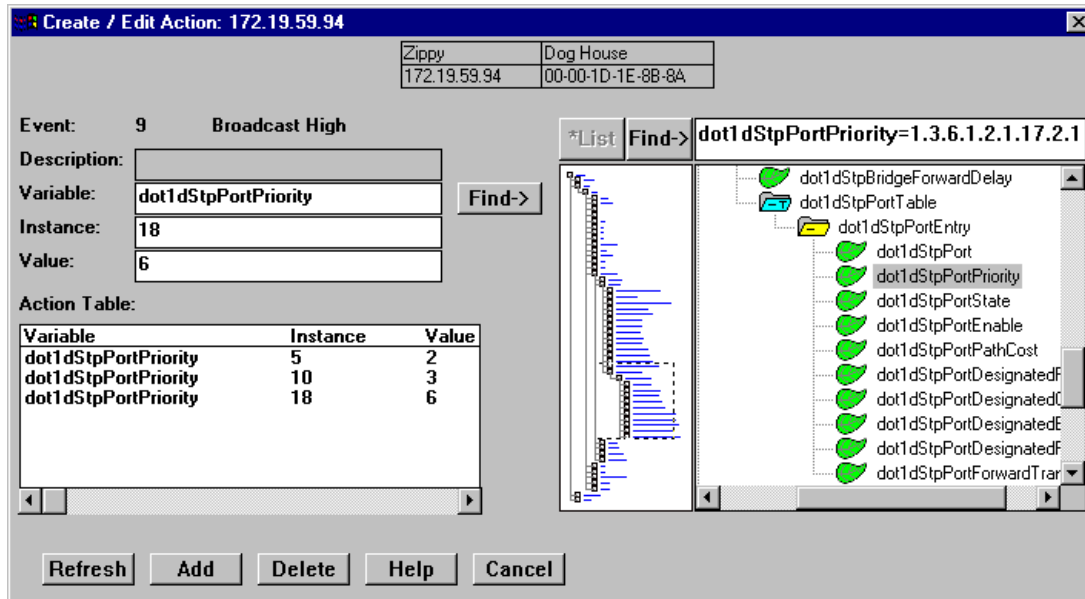
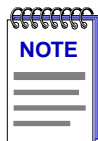


Figure 3-6. The RMON Create/Edit Actions Window



If no **Actions** button appears in the Create/Edit Events window, the selected RMON device does not support the Actions MIB. The Actions functionality will only be available for Cabletron devices, as it is supplied by a Cabletron proprietary MIB; for more information about devices which support this MIB, contact Cabletron Systems' Global Call Center.

2. The index number and description of the event with which the action or actions will be associated is displayed in the **Event:** field at the top of the window. Information in this field is not editable; to assign actions to a different event, double-click on the correct event in the Events Watch list; both the Create/Edit Events and Create/Edit Actions windows will update accordingly.
3. The **Description** field is not currently editable; future releases of SPECTRUM Element Manager will allow you to assign a descriptive label to each set of actions.
4. To select the **Variable** whose value you wish to SET, use the MIBTree panel provided on the right side of the window. (For more information about how to use the MIBTree panel, see the **MIB Tools** chapter in the **SPECTRUM**

Element Manager Tools Guide.) The display will default to the top of the tree (labeled Internet); there are three ways to locate and/or assign the correct variable:

- a. If you know the exact name of the OID whose value you wish to track, simply enter the name in the **Variable** field; to verify that you have entered the name correctly, click on **Find->** to move the MIBTree display to that OID. (If MIBTree display does not adjust to show the OID you've entered, you've entered the name incorrectly.)
- b. Use the Radar View panel located just left of the MIB Tree panel to adjust the MIB Tree display to the part of the tree that contains the variable you are interested in, then click to open the appropriate folders. (Again, see the **Tools Guide** for more details on using the Radar View.)
- c. Use the scroll bars and click to open the appropriate folders in the MIBTree panel to locate the object you wish you use; click to select it in the panel, and its name will automatically be entered in the **Variable** field.



If you select an invalid OID — that is, one which does not permit write access — the message !!Can't set action on this type!! will be displayed in the Variable field.

*If you don't know the exact spelling of the OID you wish to use for your alarm variable, and you can't find it by searching through the tree, use the MIBTree utility's Find feature to locate the OID and determine its exact spelling (and tree location). For more information on the MIBTree panel and its Find capabilities, see Chapter 3, **MIB Tools**, in the **SPECTRUM Element Manager Tools Guide**. Note that this Find feature is no longer case-sensitive.*

5. Once you have selected the object you wish to set, you must assign the appropriate instance value in the **Instance** field. If you're not sure how the object you wish to set is instanced, you can use the MIBTree utility (described in the **Tools Guide**) to query it; all available instances for the object will be displayed.
6. In the **Value** field, enter the value you wish to set for the selected object. Again, if you're not sure what the valid values are for the variable you wish to set, locate the object in the MIBTree utility and use the **Details** button to obtain more information.
7. Once you've configured your action, click on **Add**; the action will be added to the Action Table list in the lower left corner of the window. Note that the window remains open so that you may configure additional new actions or modify existing ones; selecting any action in the Action Table will display that action's parameters in the window and make them available for editing. When you have finished configuring your actions, click on **Cancel** to close the window.

Note that the Action Table will update automatically each time an action is added or deleted; use the **Refresh** button to update the table at any time.

Deleting an Alarm, Event, or Action

To delete an alarm, event, or action:

1. In the appropriate window, highlight the alarm, event, or action you wish to remove.
2. Click on **Delete** to remove. A window will appear asking you to confirm your selection; click on **OK** to delete, or on **Cancel** to cancel.

When you delete an event, be sure you edit all alarms that were pointing to that event, and assign a new valid event to those thresholds; note, too, that deleting an event automatically deletes its associated actions, as actions cannot exist in the absence of an association with an event.

Again, as a general rule, we recommend that you do *not* delete an alarm or event of which you are not the owner.

Viewing an Advanced Alarm Event Log

To view the log of occurrences for any event:

1. Highlight the event for which you wish to view the log, then click on **Event Log** at the bottom of the Advanced Alarm/Event List window; the Event Log window, [Figure 3-7](#), will appear.

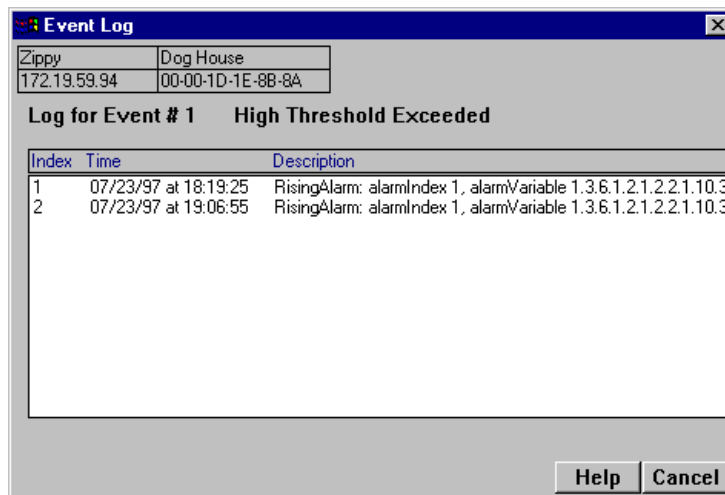


Figure 3-7. The Event Log Window

The top portion of the window contains the device information boxes, as well as the event index number and the event description; the log itself includes the following fields:

Index	This index number is not the <i>event's</i> index, but a separate index that uniquely identifies this <i>occurrence</i> of the event.
Time	Indicates the date and time of each event occurrence.
Description	Provides a detailed description of the alarm that triggered the event: whether it was a rising or falling alarm, the alarm index number, the alarm variable name and object identifier (OID), the alarmSampleType (1=absolute value; 2=delta value), the value that triggered the alarm, the configured threshold that was crossed, and the event description. Use the scroll bar at the bottom of the log to view all the information provided.

Each log will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

How Rising and Falling Thresholds Work

Rising and falling thresholds are intended to be used in pairs, and can be used to provide notification of spikes or drops in a monitored value — either of which can indicate a network problem. To make the best use of this powerful feature, however, pairs of thresholds should not be set too far apart, or the alarm notification process may be defeated: a built-in hysteresis function designed to limit the generation of events specifies that, once a configured threshold is met or crossed in one direction, no additional events will be generated until the opposite threshold is met or crossed. Therefore, if your threshold pair spans a wide range of values, and network performance is unstable around either threshold, you will only receive one event in response to what may be several dramatic changes in value. To monitor both ends of a wide range of values, set up two pairs of thresholds: one set at the top end of the range, and one at the bottom. [Figure 3-8](#) illustrates such a configuration.

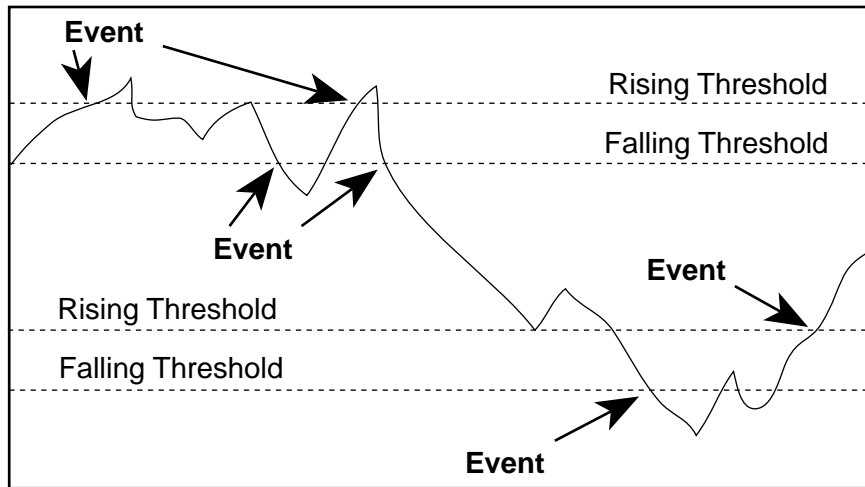
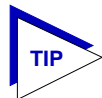


Figure 3-8. Sample Rising and Falling Threshold Pairs



The current version of the Basic Alarms window only allows you to configure a single pair of thresholds for each alarm variable on each interface; be sure to keep this hysteresis function in mind when configuring those threshold values.

Statistics

Accessing MIB-II interface or RMON statistics from the Module View; available statistics windows

Each port menu in the 9H42x-xx Module View provides two statistics selections: **Statistics** and **I/F Statistics**. Selecting the **Statistics** option will launch the highest level of statistics available for the selected interface: if the interface supports RMON, the RMON statistics window will display; if the interface does not support RMON, or if the RMON Default MIB component has been administratively disabled, the MIB-II I/F statistics window will display. Selecting the **I/F Statistics** option will always display MIB-II interface statistics, regardless of the level of RMON support available or the current administrative status of the RMON Default MIB component.



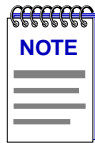
*Note that the MIB-II I/F Statistics window is also available for all port interfaces — regardless of their level of RMON support or the current administrative status of the RMON Default MIB component — via the I/F Summary window accessed from the Device menu, and via the I/F Statistics option on the bridge Port menu in the Bridge Status view. For more information about the I/F Summary window, see **Chapter 2**; for more information about the Bridge Status view, see **Chapter 5**.*

Accessing the Statistics Windows

1. Click on the desired port button from the Module View window. The Port menu will appear.
2. **For RMON statistics** (where available), click to select **Statistics**, and release. The RMON Statistics ([Figure 4-1](#)) or MIB-II Interface Statistics ([Figure 4-3, page 4-7](#)) window, as appropriate, will appear.

or

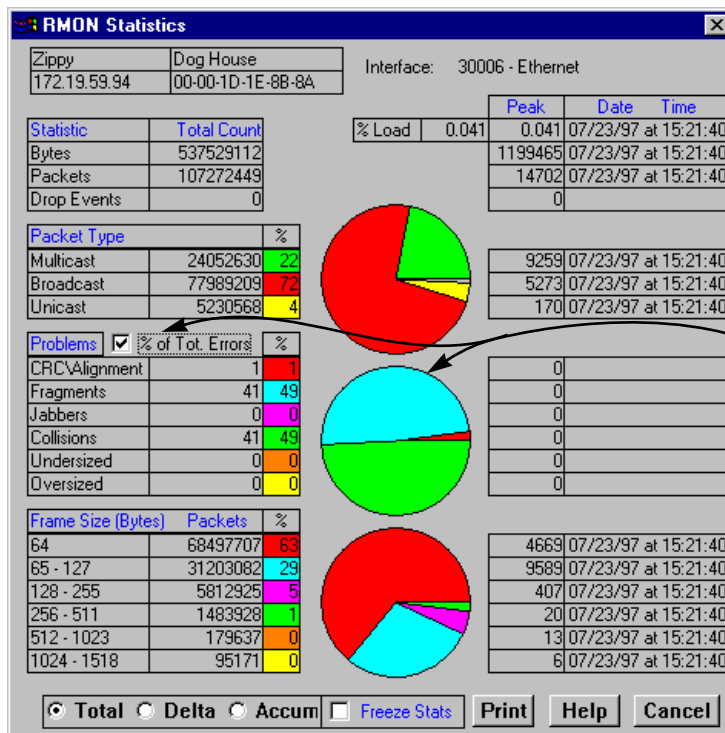
For MIB-II interface statistics, click to select **I/F Statistics**, and release. The MIB-II Interface Statistics window ([Figure 4-3, page 4-7](#)) will appear.



If the selected interface displays MIB-II I/F Statistics and you were expecting to see RMON statistics, the RMON Default MIB component may be disabled; see the **RMON User's Guide** for information on how to check (and if necessary, change) the admin status of the RMON Default MIB component.

RMON Statistics

The RMON Ethernet Statistics window (Figure 4-1) provides a detailed statistical breakdown of traffic on the monitored Ethernet network — including byte, packet, and dropped packet counts; breakdowns of the packet's address type; breakdowns of error packets; and breakdowns of packet frame sizes. Statistics are provided both numerically and graphically, and include peak values and the date and time they occurred.



The Errors pie chart will only be displayed when the **% of Tot. Errors** option is selected

Figure 4-1. The Ethernet Statistics Window

The selected interface number and its description are displayed at the top of the Statistics window. The column on the left side of the window displays each statistic's name, total count, and percentage; the column on the right displays the peak value for each statistic, and the date and time that peak occurred. Note that peak values are always Delta values; see **Viewing Total, Delta, and Accumulated Statistics**, page 4-5, for more information.

Ethernet statistics are:

Bytes

Displays the total number of bytes contained in packets processed on the network segment. This number includes bytes contained in error packets.

Packets

Displays the total number of packets processed on the network segment. Again, this number includes error packets.

Drop Events

This field indicates the number of times packets were dropped because the device could not keep up with the flow of traffic on the network. Note that this value does not reflect the number of packets dropped, but only the number of times packets were dropped.

% Load

Displays the network segment load during the sample interval, in hundredths of a percent; this percentage reflects the network segment load compared to the theoretical maximum load (10 Mbps for Ethernet; 100 Mbps for Fast Ethernet).

Packet Type

Multicast	Indicates the number of good packets processed on the network segment that were destined for more than one address. Note that this total does not include broadcast packets.
Broadcast	Indicates the number of good packets processed on the network segment that had the broadcast (FF-FF-FF-FF-FF-FF) destination address.
Unicast	Indicates the number of good packets processed on the network segment that were destined for a single address.

The percentages displayed to the right of the numerical values for these fields indicate what percentage of good packets transmitted on the network segment were multicast, broadcast, and unicast; these percentages will add up to 100. The pie chart in the center of the window provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

Problems

CRC/Alignment	Indicates the number of packets processed by the network segment that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclic Redundancy Check, or CRC error).
---------------	---

Fragments	Indicates the number of packets processed by the network segment that were undersized (less than 64 bytes in length; a runt packet) <i>and</i> had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
Jabbers	Indicates the number of packets processed by the network segment that were oversized (greater than 1518 bytes; a giant packet) <i>and</i> had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
Collisions	Indicates the total number of receive (those the device detects while receiving a transmission) and transmit (those the device detects while transmitting) collisions detected on the network segment.
Undersized	Indicates the number of packets processed by the network segment that contained fewer than 64 bytes (runt packets) but were otherwise well-formed.
Oversized	Indicates the number of packets processed by the network segment that contained more than 1518 bytes (giant packets) but were otherwise well-formed.

In their default state, the percentages displayed to the right of the numerical values for these fields indicate what percentage of **total packets** transmitted on the network segment were of the noted type. If you select the **% of Tot. Errors** option by clicking the mouse button in the check box, the percentages will indicate what percentage of **problem, or error, packets** transmitted on the network segment were of the noted type; these percentages will add up to 100. (The **% of Tot. Errors** option is active if there is an X in the check box.) The pie chart in the center of the window provides a graphical view of the selected percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

Frame Size (Bytes) Packets

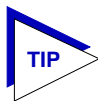
The Frame Size (Bytes) Packets fields indicate the number of packets (including error packets) processed by the network segment that were of the noted length, excluding framing bits but including frame check sequence bits. Packet sizes counted are:

- 64
- 65-127
- 128-255
- 256-511
- 512-1023
- 1024-1518

The percentages displayed to the right of the numerical values for these fields indicate what percentage of all packets transmitted on the network segment were of the noted size. Unless the network segment has experienced a significant number of runts and/or giants (which are not counted in this group), these percentages will add up to 100. The pie chart in the center of the window provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

Viewing Total, Delta, and Accumulated Statistics

By using the **Total**, **Delta**, and **Accum** radio buttons located at the bottom of the Statistics window, you can choose whether to view the total statistics count (since the last time the device was initialized), the statistics count during the last polling interval, or a fresh accumulation of statistics begun when the **Accum** button was selected.

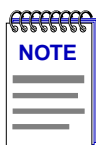


*The statistics windows use the polling interval you have set for the monitored device via the Device Properties window. See your **Installing and Using** guide for more information on setting the polling interval.*

To choose **Total**, **Delta**, or **Accum**:

1. Click on the **Total** radio button; after the completion of the current polling cycle plus one complete polling cycle, the screen will display the total count of statistics processed since the entry was created or since the device was last initialized, whichever is most recent. These totals are updated after each polling cycle.
2. Click on the **Delta** radio button; after the completion of the current polling cycle plus two more polling cycles, the screen will display the count of statistics processed during the last polling interval. These counts will be refreshed after each polling cycle.
3. Click on the **Accum** radio button; after the completion of the current polling cycle plus two more polling cycles, the screen will display a fresh cumulative count of statistics. Note that making this selection does **not** clear device counters; you can still re-select **Total** for the total count since the device was last initialized.

Note that switching the statistics displays among **Total**, **Delta**, and **Accum** does not effect the displayed peak values, as peak values are always **Delta** values.



If you reset your device, you must first close, then re-open the Statistics window to refresh peak values.

To temporarily freeze the statistics display, select the **Freeze Stats** option; in this mode, statistics will continue to be collected, but the display will not update. To resume normal updates, click again to de-select the freeze option.

Printing Statistics

The **Print** button located at the bottom of the Statistics window allows you to print the current snapshot of statistical data. When you select **Print**, a standard Windows print window like the sample shown in [Figure 4-2](#) will appear.

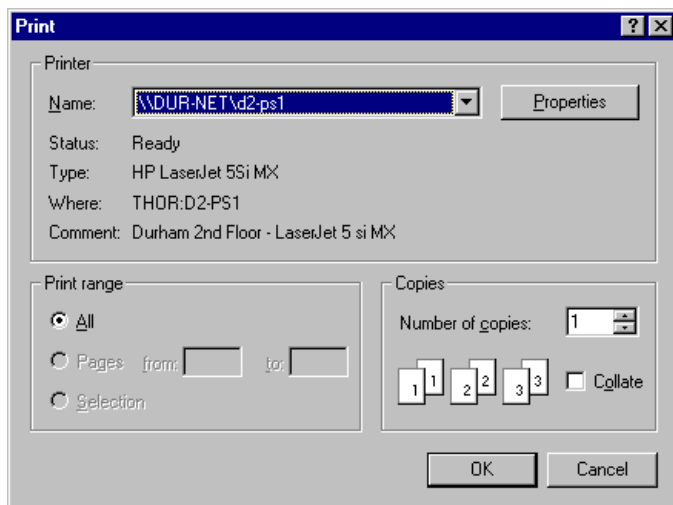
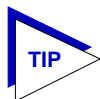


Figure 4-2. Standard Print Window

Adjust printer settings as required, then click **OK**. (For more information on the appropriate printer settings, consult your *Microsoft Windows User's Guide*.)

Interface Statistics

The Interface (IF) Statistics window ([Figure 4-3](#)) provides MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for any port interface on the selected 9H42x-xx module.



*Remember, this window can always be launched from the **I/F Statistics** option on the Module View port menus; it may also be launched from the **Statistics** option if the selected interface does not support RMON or if the RMON Default MIB component has been administratively disabled. This window is also available for all port interfaces via the I/F Summary window (described in [Chapter 2](#)) or the bridge port menus in the Bridge Status view (see [Chapter 5](#)).*

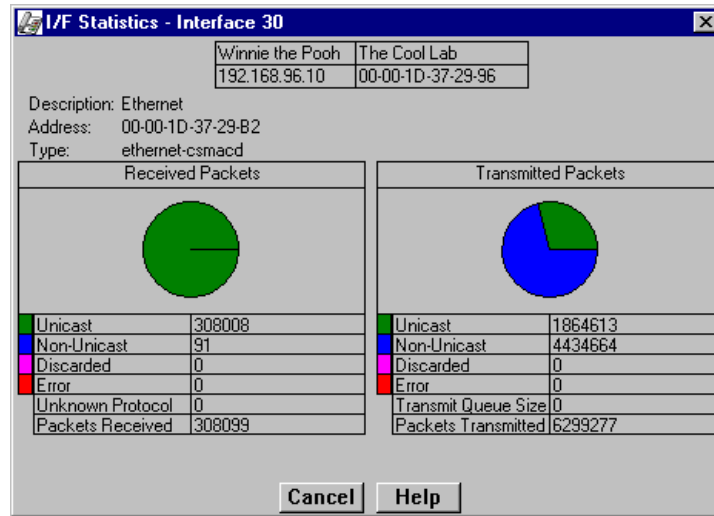
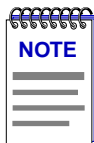


Figure 4-3. Interface Statistics Window



Because of the mismatch between the number of physical interfaces on the device and the number of interfaces performing bridging, the physical indexing of interfaces (the MIB-II *ifIndex*) does not match the indexing of ports with respect to the bridge. For all 9H42x-xx modules, bridge port indexing begins at index 1 with the INB interface (which has an *ifIndex* of 5); the remaining bridge ports are indexed sequentially from there.

Three informational fields appear in the upper portion of the window:

Description

Displays the interface description for the currently selected port: Ethernet or INB.

Address

Displays the MAC (physical) address of the selected port.

Type

Displays the interface type of the selected port: ethernet-csmacd or other (for the INB interface). Note that there is no type distinction between Ethernet and Fast Ethernet.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast

Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast

Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The non-unicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded

Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges. Consult the Cabletron Systems' *Network Troubleshooting Guide* for more information.

These statistics are displayed in the pie chart, color-coded magenta.

Error

Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol (Received only)

Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received (Received only)

Displays the number of packets received by the selected interface.

Transmit Queue Size (Transmit only)

Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the 9H42x-xx module will begin to discard packets.

Packets Transmitted (Transmit only)

Displays the number of packets transmitted by this interface.

Bridging

Bridge management overview; the Bridge Status window; bridge Performance Graphs; changing bridge Spanning Tree parameters; configuring the Filtering Database; setting duplex modes; using the port Source Addressing window

Bridging Basics

When configured to operate as a traditional switch, your 9H42x-xx Fast Ethernet SmartSwitch modules have the ability to act as 802.1d Transparent Bridges to direct traffic between the network segments connected to their front panel and the interface to the INB backplane.

Bridges are used in local area networks to connect two or more network segments and to control the flow of packets between the segments. Ideally, bridges forward packets to another network segment only when necessary.

Bridges are also used to increase the fault tolerance in a local area network by creating redundant bridge paths between network segments. In the event of a bridge or bridge segment failure, an alternate bridge path will be available to network traffic, without significant interruption to its flow.

The method a bridge uses to forward packets, choose a bridge path, and ensure that a sending station's messages take only one bridge path depends on the bridge's type: Transparent (generally used in Ethernet or FDDI environments) or Source Routing (generally used in Token Ring environments).

Transparent bridging relies on a "Filtering Database" to make forwarding decisions. The source addresses of data coming into each bridge interface are read and stored in a Filtering Database that associates each address with the interface it was detected on. When a packet is received by the bridge, it can then compare the destination address of the packet to the addresses in the Filtering Database, and determine which bridge interface to send the packet to.

In Source Route bridging, the source node sends "explorer" packets to a destination node that pass through a bridged network. Each bridge that sees the explorer packet will append Routing Information (in the form of LAN segment numbers) to it. When the destination node receives these explorer packets, it will

return a response to the source node that contains the route information field indicating which bridge paths the explorer packets took. In future communication between the two nodes, the original source node will append the best route to the destination node in a Routing Information Field (RIF) of its data frames, so that a bridge on the network will simply have to examine the RIF to verify whether it is a part of the route process.

More on Transparent Bridging

Transparent bridges are most common in Ethernet networks. Individual Transparent bridges monitor packet traffic on attached network segments to learn their network segment location in terms of which bridge port receives packets originating from a particular station (determined via the packet's Source Address field). This information gets stored in the bridge's Filtering Database. When in the Forwarding state, the bridge compares a packet's destination address to the information in the Filtering Database to determine if the packet should be forwarded to another network segment or filtered (i.e., not forwarded). A bridge filters a packet if it determines that the packet's destination address exists on the same side of the bridge as the source address.

Transparent bridges in a network communicate with one another by exchanging Bridge Protocol Data Units, or BPDUs, and collectively implement a Spanning Tree Algorithm (STA) to determine the network topology, to ensure that only a single data route exists between any two end stations, and to ensure that the topology information remains current.

An Overview of Bridge Management

With SPECTRUM Element Manager, you can view and manage bridging across the 9H42x-xx module — and at each bridging interface — by using the following windows:

- The **Bridge Status** window provides you with basic information about the current status of the 9H42x-xx module's bridging interfaces, and allows you to enable or disable bridging at each interface of the switch. The Bridge Status window also lets you access further windows to configure bridging at the 9H42x-xx module.
- The **Performance Graph, Statistics, and I/F Statistics** windows graphically display the traffic passing between bridged networks, and let you compare and contrast traffic processed by each interface. Performance graphs are described beginning on [page 5-7](#); the statistics windows are described in **Chapter 4**.
- The **Spanning Tree** window shows bridge port information and protocol parameters relating to the Spanning Tree Algorithm (the method of determining the controlling bridge when a series of bridges are placed in parallel).

- With the **Filtering Database** window, you can see the contents of the Static and Learned databases — the two address databases which construct the IEEE 802.1d Source Address Table. The switch uses the contents of these databases to make its packet filtering and forwarding decisions when using 802.1d bridging. You can configure entries in these databases to increase bridging efficiency across your network.
- The **Port Source Addressing** window displays the contents of the 9H42x-xx switch's 802.1d Bridge Filtering Database with respect to a selected interface. This will display the source MAC addresses that have been detected by the interface as it forwards data across the network. The window also lets you set the ageing timer that controls how long an inactive MAC address will continue to be stored in the Source Address Database before being aged out.
- The bridge-level **Duplex Modes** and port-level **Configuration** options allow you to set Duplex Mode operation for standard Ethernet interfaces; the port-level Configuration option for Fast Ethernet interfaces also allows you to configure parameters related to auto-negotiation. The Duplex Modes window is described beginning on [page 5-25](#); the port configuration windows are described in **Chapter 2**.

The following sections detail how to use each of the bridge management windows.

The Bridge Status Window

The Bridge Status window provides you with basic information about the current status of bridging across your device. Color-coding of each port display allows you to quickly ascertain the status of each interface. The Bridge Status window also lets you access further windows to control bridging at your 9H42x-xx module.

To access the Bridge Status window from the Module View:

1. Click on **Device** to display the Device menu.
2. Click to select **Bridge Status....** The Bridge Status window, [Figure 5-1](#), will appear.

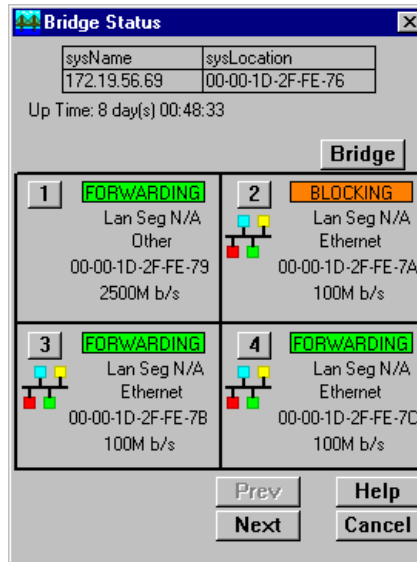


Figure 5-1. The Bridge Status Window

The Bridge Status window provides the following information for each individual bridging interface; the **Prev** and **Next** buttons allow you to scroll the display to show all available bridge port interfaces.

Up Time

At the top of the Bridge Status window, you can see the time period (in a days, hours, minutes, seconds format) that has elapsed since the 9H42x-xx module was last reset or initialized.

Spanning Tree State

Indicates the state of bridging over each port interface. Note that this state (and its corresponding color-code) will also be reflected on the Bridge port status display in the Module View window. Possible bridge states and their corresponding colors are:

- **Forwarding** (green) — the port is on line, and is configured by Spanning Tree Algorithm to forward frames to and from its attached network.
- **Disabled** (blue) — bridging at the port has been disabled by management; no traffic can be received or forwarded, including configuration information for the bridged topology.
- **Listening** (magenta) — this bridge port is not adding information to the Filtering Database. The port is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the Forwarding state.

- **Learning** (magenta) — the Forwarding database is being created or the Spanning Tree Algorithm is being executed due to a network topology change; the port is monitoring network traffic, learning network addresses.
- **Blocking** (orange) — Spanning Tree Algorithm has configured this port to block (filter) frames to prevent redundant data loops in the bridged network; the port can't receive or forward traffic. Bridge topology information will be forwarded by the port.
- **Broken** (red) — the physical interface has malfunctioned.

Interface Type

Indicates the interface type which applies to each bridge port interface. The interface type (ifType) is a mandatory object type from the SNMP MIB-II Interface (IF) Group.

Bridge Address

Indicates the physical (MAC) address of the bridge port.

Interface Speed

Indicates the theoretical maximum speed of the selected interface: 10 Mbits for standard Ethernet; 100 Mbits for Fast Ethernet; 2500 Mbits for the INB.

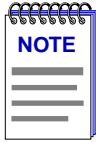
Accessing Other Management Options from the Bridge Status Window

At the top of the Bridge Status window, you can click on **Bridge** to access a menu that provides other bridge management options:

- A Bridge Performance Graph that displays statistics for traffic across the entire bridge (see **Bridge Statistics**, page 5-7).

A Performance Graph window is also available for each individual interface, by clicking on a port index button to display the port level management options (see **Bridge Statistics**, page 5-7).

- The Spanning Tree window, which allows you to set the Spanning Tree Algorithm parameters for bridging on your 9H42x-xx module (see **Bridge Spanning Tree**, page 5-11).
- The Filtering Database window, which lets you configure the bridge's acquired and permanent filtering databases to filter or forward traffic across the bridge port interfaces present on the selected 9H42x-xx module (see **Filtering Database**, page 5-19).
- The Duplex Modes window, which allows you to configure duplex mode (on or off) for standard Ethernet interfaces; see **Duplex Modes**, page 5-25, for details.



For Fast Ethernet interfaces, you configure the Duplex Mode (as well as speed and parameters related to auto-negotiation) via the Port Configuration window available from the individual bridge port menus.


Enabling and Disabling Bridging

When you disable a bridge port, you disconnect that port's network from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge and other networks connected to the bridge. When you enable a port, the port moves from the Disabled state through the Listening and Learning states to the Forwarding or Blocking state (as determined by Spanning Tree).

Enabling and Disabling Individual Interfaces

There are two ways to disable an individual port interface:

from the Bridge Status window:

1. Click on the desired **Port** button () to display the port menu.
2. Drag down to **Enable** to restart bridging on the selected interface, or **Disable** to halt bridging across the selected interface.


from the Module View window:

1. Click on the appropriate port display to access the Port menu.
2. Drag down to **Enable** to restart bridging on the selected interface, or **Disable** to halt bridging across the selected interface.

Enabling and Disabling All Installed Interfaces

Similarly, there are two ways to disable bridging across all interfaces on the 9H42x-xx module:

from the Bridge Status window:

1. Click on  to display the Bridge Status menu.
2. Drag down to **Enable Bridge** to enable bridging across all installed interfaces, or to **Disable Bridge** to disable bridging across all installed interfaces.

from the Module View window:

1. Click on the **Bridge** label just above the port status displays; the Bridge menu will appear.
2. Drag down to **Enable Bridge** to enable bridging across all interfaces, or to **Disable Bridge** to disable bridging across all interfaces.

Bridge Statistics

There are three statistics windows available for the 9H42x-xx module: the **Statistics** window (accessible from both the Module View and Bridge Status view port menus) displays any available RMON-based statistics; the **I/F Statistics** window (also accessible from the Module View and Bridge Status view port menus) displays MIB-II interface statistics; and the **Performance Graphs** display statistics related to the bridging function being performed either by an individual interface, or by the device as a whole. The Statistics and I/F Statistics windows are described in **Chapter 4**; information about Performance Graphs follows.

Performance Graphs

Bridge Performance Graphs provide a color-coded strip chart that shows you the traffic being bridged through all networks or an individual network connected to the selected 9H42x-xx module. You can configure the display to show frames filtered, forwarded, and/or transmitted, as well as the number of errors. The graph has an x axis that indicates the 60 second interval over which charting occurs continuously; the y axis measures the number of packets or errors that are processed by the module as a whole or by one of its bridging interfaces.

You can select the statistics you wish to monitor by using the menu buttons provided; when you change Performance Graph parameters, the graph will refresh and generate a strip chart based on the newly defined parameters.

To access the collective Bridge Performance Graph window:

1. From the Bridge Status window, click on **Bridge** to display the Bridge Status menu.

or

From the Module View window, click on the **Bridge** label just above the port status display; the Bridge menu will appear.

2. Click to select **Performance Graph...**, and release. The Bridge Performance Graph window, [Figure 5-2](#), will appear. (The individual port Bridge Performance Graph windows are similar, except that they display a graph applicable to the selected interface.)

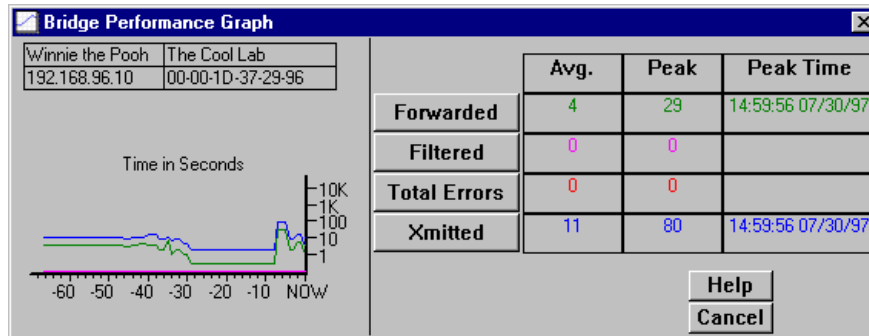


Figure 5-2. Bridge Performance Graph

To access the individual bridge port interface Performance Graph windows:

1. From the Bridge Status window, click on the appropriate **port** button (**1**) to display the port menu.

or

From the Module View window, click on the appropriate **Port Index** on the module display; the Port menu will appear.

2. Click to select **Performance Graph...**, and release. The port-level Bridge Performance Graph window will appear.

For each chosen statistic, Performance Graphs display both average and peak activity, as well as the date and time the peak values were recorded; average values are also displayed graphically.

The Average statistics are updated every two seconds, as averaged over the previous four two-second intervals; the graphical display also updates at two-second intervals. For the first 60 seconds of graphing, you will note the graph lines extending as each interval's data is added to the graph. Once the first 60 seconds has passed, the newest data is added at the right edge of the graph, and the oldest data is scrolled off to the left.

Available performance statistics are:

Forwarded (Green)

Forwarded The number of frames forwarded by the bridge, at the device or port level.

Nothing The Frames Forwarded function is currently not measuring any statistics.

Filtered (Magenta)

Filtered	The total number of frames filtered by the bridge, at the device or port level.
Nothing	The Filtered scale is not currently measuring the number of packets filtered by the bridge.

Total Errors (Red)

Total Errors	The total number of errors experienced by all bridging interfaces on the selected 9H42x-xx module, or by an individual bridge interface.
Nothing	The Errors scale is currently not measuring error packets coming through the device as a whole or a single port.

Xmitted (Blue)

Xmitted	The total number of frames transmitted by the selected bridge interface, or by all bridge interfaces.
Nothing	The Xmitted scale is not currently measuring the number of packets filtered by the bridge or the selected individual interface.

Configuring the Bridge Performance Graphs

To configure the Bridge Performance Graph:

1. Using the mouse, click on **Forwarded** (with green statistics to the right). The Forwarded menu will appear. Click on the desired mode.
2. Click on **Filtered** (with magenta statistics to the right). The Filtered menu will appear. Click on the desired mode.
3. Click on **Total Errors** (with red statistics to the right). The Errors menu will appear. Click on the desired mode.
4. Click on **Xmitted** (with blue statistics to the right). The Xmitted menu will appear. Click on the desired mode.

Once you have selected a new mode, it will appear in its respective button, and after the next poll the Performance Graph will refresh and begin to measure using the new mode.

Using Source Addressing

The Source Addressing feature allows you to display a list of the MAC addresses communicating through each bridge port interface available on the selected 9H42x-xx module.

To access the Source Addressing windows:

1. From the Bridge Status window, click on the appropriate **port** button (**1**) to display the port menu.

or

From the Module View window, click on the appropriate **Port Index** on the module display; the Port menu will appear.

2. Drag down to **Source Addressing...**, and release. The Port X Source Addresses window, [Figure 5-3](#), will appear.

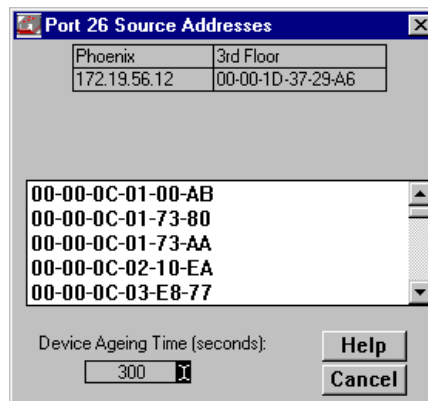



Figure 5-3. Bridge Port Source Address Window

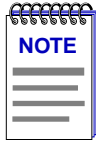
The Port Source Addresses window displays the MAC addresses of all devices that have transmitted packets that have been forwarded through the selected bridging interface during the last cycle of the Filtering Database's defined ageing timer (learned addresses that have not transmitted a packet during one complete cycle of the ageing timer are purged from the Source Address Table). For more information on the Filtering Database, see [Filtering Database](#) on [page 5-19](#).

Altering the Ageing Time

To alter the Source Address Ageing Time:

1. Click on the I-bar cursor in the Device Ageing Time field; a window will appear with a text field for entering a new ageing time.

2. Type in the new Ageing Time, in seconds, then click on . The allowable range is 10 to 1,000,000 seconds.



Note that the Source Addresses Ageing Time is the same as the Ageing Time displayed (and configured) via the Filtering Database window; setting the Ageing Time in the Source Addresses window also changes the time in the Filtering Database window, and vice versa.

Bridge Spanning Tree

The Bridge Spanning Tree window allows you to display and modify the 9H42x-xx module's bridge port information and protocol parameters relating to the Spanning Tree Algorithm.

In a network design with multiple transparent bridges placed in parallel (i.e., attached to the same local network segment), only a single bridge should forward data through the LAN, leaving the remaining bridges on the segment in a standby state so that another can assume the bridging responsibility should the current active bridge go down. The Spanning Tree Algorithm (STA) is the method that bridges use to communicate with each other to ensure that only a single data route exists between any two end stations.

In Transparent bridging, Spanning Tree *must* be used to prevent data loops (since in an Ethernet environment, a packet propagated down multiple paths would cause higher volumes of traffic and collisions that would cripple a network that relies on carrier sense and collision detection). Spanning Tree selects a controlling Root Bridge and Port for the entire bridged local area network, and a Designated Bridge and Port for each individual network segment. The Root bridge is the one that selects one of two or more available bridge paths between two end stations, basing its decision on factors associated with each of the bridges in the path. A Designated Port/Bridge for a network segment relays frames toward the Root Bridge, or from the Root Bridge onto the network segment. When data passes from one end station to another across a bridged local area network, it is forwarded through the Designated Bridge/Port for each network segment towards the Root Bridge, which in turn forwards frames towards Designated Bridges/Ports on its opposite side.

During the Root Bridge selection process, all bridges on the network communicate STA information via Bridge Protocol Data Units (BPDUs). It is with BPDUs that the bridges collectively determine the current network topology and ensure that all bridges have current topology information.

To access the Bridge Spanning Tree window:

1. From the Bridge Status window, click on **Bridge** to display the Bridge Status menu.

or

From the Module View window, click on the **Bridge** label just above the port status display; the Bridge menu will appear.

2. Click on **Spanning Tree....** The Bridge Spanning Tree window, [Figure 5-4](#), will appear.

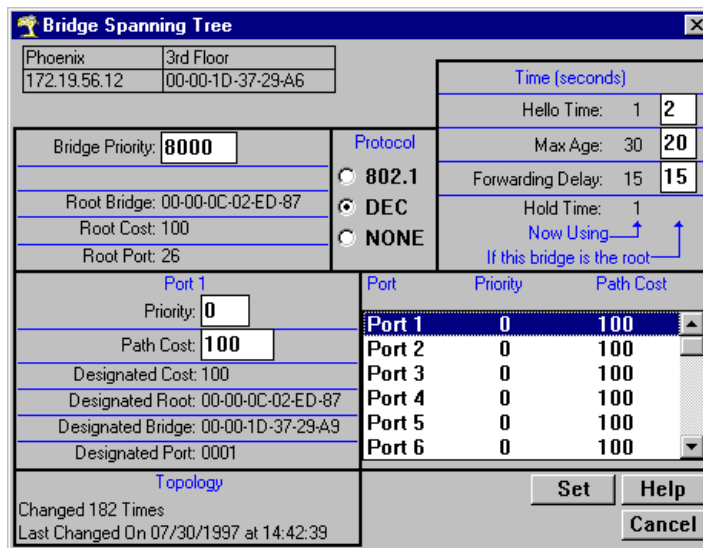


Figure 5-4. Bridge Spanning Tree Window

Viewing Spanning Tree Parameters

The Bridge Spanning Tree window displays current STA parameters and allows you to alter parameters for the bridge as a whole and/or for each individual bridging interface.

The currently selected bridging interface is highlighted in the lower right quadrant of the window. To alter the parameters of another interface, click on the appropriate **Port X** name listed in the quadrant.

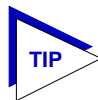
Bridge-level Parameters

The Bridge Spanning Tree window provides the following bridge-level information:

Bridge Priority

This field displays the “priority” component of the 9H42x-xx module’s unique bridge identifier. The Spanning Tree Algorithm assigns each bridge a unique identifier, which is derived from the bridge’s MAC address and the Priority. The bridge with the lowest value of bridge identifier is selected as the Root. A lower priority number indicates a higher priority; a higher priority enhances a bridge’s chance of being selected as the Root.

You can edit this text box to change network topology, if needed. The default value is 8000 (hex value 80-00).



Part of a bridge’s Identifier is based on its MAC address. In most network installations, the difference in performance levels between bridges may be negligible. You may, however, find your data bottle-necked in installations where both a low-performance bridge and a high-performance bridge are attached to the same LAN segment and the two (or more) bridges have the same Priority component set (e.g., at the default 8000 Hex). In such a scenario you may want to alter the Priority component of the higher performance bridge to ensure that it becomes root for the segment (or overall root). Remember, if Priority components are equal the bridge on the segment with the lowest Hex value of MAC address would have a better chance of being selected as the root bridge — as it would have a lower Bridge Identifier. If your bridges come from multiple vendors, they will have different MAC address values (e.g., Cabletron devices have a lower MAC address than 3Com devices); if they come from the same vendor, the bridge with the earlier manufacture date will be likely to have the lower MAC address value.

Root Bridge

Displays the MAC address of the bridge that is currently functioning as the Root Bridge.

Root Cost

Indicates the cost of the data path from this bridge to the Root Bridge. Each port on each bridge adds a “cost” to a particular path that a frame must travel. For example, if each port in a particular path has a Path Cost of 1, the Root Cost would be a count of the number of bridges along the path. (You can edit the Path Cost of bridge ports as described later.) The Root Bridge’s Root Cost is 0.

Root Port

This field displays the identifier (the physical index number) assigned to the bridge port that has the lowest cost path to the Root Bridge on the network. If the 9H42x-xx module itself is currently the Root Bridge, this field will read 0.

Protocol

Displays the Spanning Tree Algorithm Protocol type the 9H42x-xx module is currently using. The choices are:

- 802.1
- DEC (DEC Lanbridge 100)
- None

The following four fields display values used for various Spanning Tree timers in the course of normal operations. Three of these values — Hello Time, Max Age, and Forwarding Delay — are configurable; the values currently in use are those which have been set at the Root Bridge. Both the values currently in use and those which would be used if the monitored 9H42x-xx module were to become the root bridge are displayed in the upper-right corner of the window. Note that Hold Time is not configurable; this is a fixed value and cannot be changed.

Hello Time

This parameter indicates, in seconds, the length of time the Root Bridge (or bridge attempting to become the Root) waits before resending Configuration BPDUs. The range for this field is 1 to 10 seconds, with a default value of 2 seconds. The Root Bridge sets the Hello Time.

Max Age

This parameter displays the bridge's BPDU ageing timer. This controls the maximum time a BPDU can be retained by the bridge before it is discarded. During normal operation, each bridge in the network receives a new Configuration BPDU before the timer expires. If the timer expires before a Configuration BPDU is received, it indicates that the former Root is no longer active. The remaining bridges begin Spanning Tree operation to select a new Root. The current Root Bridge on the network sets the Max Age time. The range for this field is 6 to 40 seconds, with a default value of 20 seconds.

Forwarding Delay

This parameter displays the time period which elapses between states while the bridge is moving to the Forwarding state. For example, while moving from a Blocking to a Forwarding state, the port first moves from Blocking to Listening to BPDU activity on the network, remains there for the Forward Delay period, then moves to the Learning State (and remains in it for the Forward Delay period), and finally moves into a Forwarding state. This timer is set by the Root Bridge. During a topology change, the Forward Delay is also used as the Filtering Database Aging Time (refer to **Filtering Database**, [page 5-19](#)), which ensures that the Filtering Database maintains current topology information.

Hold Time

This parameter displays, in seconds, the minimum time that can elapse between the transmission of Configuration BPDUs through a bridge port. The Hold Time ensures that Configuration BPDUs are not transmitted too frequently through any bridge port. Receiving a BPDU starts the Hold Timer. After the Hold Timer

expires, the port transmits its Configuration BPDU to send configuration information to the Root. The Hold Time is a fixed value, as specified by the IEEE 802.1d specification.

Port-specific Parameters

The following fields are applicable to each bridge port interface present on the selected 9H42x-xx module:

Priority

If two or more ports on the same bridge are connected to the same LAN segment, they will receive the same Root ID/Root Cost/Bridge ID information in Configuration BPDUs received at each port. In this case, the BPDU's Port ID information — the transmitting port's identifier and its manageable Priority component — is used to determine which is the Designated Port for that segment.

A lower assigned value gives the port a higher Priority when BPDUs are compared. The allowable range is 0-FF hexadecimal (0-255 decimal); the default is 80 hexadecimal.

Path Cost

Displays the cost that this port will contribute to the calculation of the overall Root path cost in a Configuration BPDU transmitted by this bridge port. You can lower a port's Path Cost to make the port more competitive in the selection of the Designated Port – for example, you may want to assign a lower path cost to a port on a higher performance bridge. The allowable range is 1 to 65535.

Designated Cost

Displays the cost of the path to the Root Bridge of the Designated Port on the LAN to which this port is attached. This cost is added to the Path Cost to test the value of the Root Path Cost parameter received in Configuration BPDUs.

Designated Root

Displays the unique bridge identifier of the bridge that is assumed to be the Root Bridge.

Designated Bridge

Displays the network address portion of the Bridge ID (MAC address/priority component) for the bridge that is believed to be the Designated Bridge for the LAN associated with this port.

The Designated Bridge ID, along with the Designated Port and Port Identifier parameters for the port, is used to determine whether this port should be the Designated Port for the LAN to which it is attached. The Designated Bridge ID is also used to test the value of the Bridge Identifier parameter in received BPDUs.

Designated Port

Displays the network address portion of the Port ID (which includes a manageable Priority component) of the port believed to be the Designated Port for the LAN associated with this port.

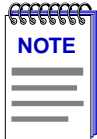
The Designated Port ID, along with the Designated Bridge and Port Identifier parameters for the port, is used to determine whether this port should be the Designated Port for the LAN to which it is attached. Management also uses it to determine the Bridged LAN topology.

Topology

This indicates how many times the bridge's Topology Change flag has been changed since the 9H42x-xx module was last powered-up or initialized. The Topology Change flag increments each time a bridge enters or leaves the network, or when the Root Bridge ID changes.

Changing Bridge Spanning Tree Parameters

The Bridge Spanning Tree window allows you to update the following parameters for the 9H42x-xx module. When you have finished making changes to the following individual parameters, you must click on at the bottom of the Spanning Tree window to write the changes to the device.



Any values you set at the bridge will cause a Topology Change flag to be issued in the next Configuration BPDUs it transmits. This will cause the bridged network to immediately recalculate Spanning Tree and change topology accordingly.

Changing Bridge Priority

To change the part of the bridge address that contains the identifier used in the Spanning Tree Algorithm for priority comparisons:

1. Highlight the **Bridge Priority** field.
2. Enter the new identifier, in hexadecimal format; the allowed range is 0-FFFF hexadecimal.
3. Click on .

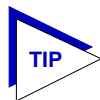
The selected Bridge Priority will be applied to the bridge (a lower number indicates a higher priority in the root selection process).

Changing the Spanning Tree Algorithm Protocol Type

To change the type of protocol used in Spanning Tree:

1. Click the mouse on the appropriate option button: **IEEE 802.1**, **DEC**, or **None**.
2. Click on .

The selected Spanning Tree Algorithm protocol type will be applied to the bridge. If you selected None, the Spanning Tree Algorithm will be disabled (if it already was enabled). If STA Protocol Type was changed from None to IEEE 802.1 or DEC, you must restart the bridge for the newly selected STA protocol to be applied.



If your network does not have redundant bridged paths, turning off Spanning Tree can improve network performance by cutting down on management (BPDU) traffic.



All bridges in a network must use the same Spanning Tree version. Mixing Spanning Tree Algorithm protocols will cause an unstable network.

Changing Hello Time

If the bridge is the Root Bridge, or is attempting to become the Root, and you want to change the length of time the bridge waits between sending configuration BPDUs:

1. Highlight the **Hello Time** field, and type in a new value.
2. Click on .

The IEEE 802.1d specification recommends that Hello Time = 2 seconds; the allowable range is 1 to 10 seconds.

Changing Max Age Time

If the 9H42x-xx module is the Root Bridge or attempting to become the Root, and you want to change the maximum time that bridge protocol information will be kept before it is discarded:

1. Highlight the **Max Age** field, and type in a new value.
2. Click on .

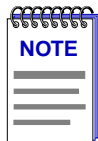
The IEEE 802.1d specification recommends that Max Age = 20 seconds; the allowable range is 6 to 40 seconds.

Changing Forwarding Delay Time

If the 9H42x-xx module is the Root Bridge or attempting to become the Root, and you want to change the time period the bridge will spend in the Listening state (e.g. either listening to BPDU activity on the network while moving from the Blocking to the Learning state or in the Learning state while the bridge is moving from the Listening to the Forwarding state):

1. Highlight the **Forwarding Delay** field, and type in a new value.
2. Click on .

The IEEE 802.1d specification recommends that Forward Delay = 15 seconds; the allowable range is 4 to 30 seconds.



To ensure proper operation of the Spanning Tree Algorithm, the IEEE 802.1d specification recommends that you always observe the following relationship between Forwarding Delay and Max Age:

$$2 \times (\text{Forwarding Delay} - 1.0) \geq \text{Max Age}$$

Changing Port Priority

To change the part of the Port Priority used in priority comparisons:

1. If necessary, select the desired port by clicking the mouse to highlight the port in the lower right quadrant of the window. The lower left quadrant of the window will now allow you to edit parameters for the selected port.
2. Highlight the port **Priority** field, and enter the new priority identifier. Only valid hexadecimal numbers (0 to FF) are allowed in this field. The default is 80 hexadecimal.
3. Click on . The new port priority will be saved.

Changing Path Cost

To change the Path Cost:

1. If necessary, select the desired port by clicking the mouse to highlight the port in the lower right quadrant of the window. The lower left quadrant of the window will now allow you to edit parameters for the selected port.
2. Highlight the **Path Cost** field, and type in a new value from 1 to 65535 decimal (default is 100 decimal).
3. Click on .

The new path cost will be applied to the port.

Filtering Database

When the 9H42x-xx switch is using Transparent Bridging, the Filtering Database, which makes up the IEEE 802.1d Source Address Table, is used to determine which frames will be forwarded or filtered between the 9H42x-xx module's bridging interfaces.

Transparent bridges like the 9H42x-xx use the **Filtering Database** to determine a packet's route through the bridge. During initialization, a bridge copies the contents of its Permanent Database to the Filtering Database. Next, the bridge learns network addresses by entering the source address and port association of each received packet into the Filtering Database. When in the Forwarding state, the bridge examines each received packet and compares the destination address to the contents of the Filtering Database. If the destination address is located on the network from which the packet was received, the bridge filters (does not forward) the packet. If the destination address is located on a different network, the bridge forwards the packet to the appropriate network. If the destination address is not found in the Filtering Database, the bridge forwards the packet to all networks. To keep Filtering Database entries current, older entries are purged after a period of time, which is called the Dynamic Ageing Time.

Entries to the Source Address Table are one of four types: **Static**, **Permanent**, **Dynamic**, or **Learned**.

- **Static** entries are addresses that you add to the Static Database (via the Filtering Database window). These entries are not subject to the ageing timer, and will remain in the Source Address Table until the 9H42x-xx module is shut down.
- **Permanent** entries are also addresses that you add to the Static Database (via the Filtering Database window); once classified as permanent, these are stored in the device's battery-backed RAM and are preserved between power-up cycles.
- **Dynamic** entries are addresses that you add to the Static Database (via the Filtering Database window). These entries are subject to the Ageing Timer, and will be automatically deleted if they do not transmit data during one complete timer cycle. You can set the ageing timer via the Ageing Time field in the Filtering Database window.
- **Learned** entries are addresses that are added to the Learned Database through the bridge's learning process. Like Dynamic entries, these entries are subject to the Ageing Timer, and will be automatically deleted if they do not transmit data during one complete timer cycle.

Learned address entries are divided into two types: **Learned** and **Self**. Address entries classified as **Learned** have transmitted frames destined for a device attached to a network segment installed in the 9H42x-xx module; address entries classified as **Self** are those that have sent a frame with a source address of one of the 9H42x-xx module's available bridge port interfaces.

At the Filtering Database window (Figure 5-5), you can view the number of entries of each type: Permanent, Static, Dynamic, or Learned.

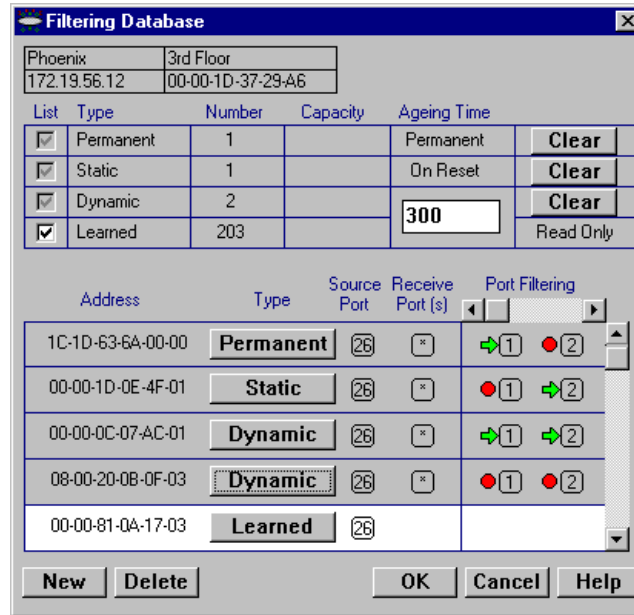
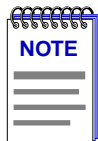


Figure 5-5. The Filtering Database Window



When you first initialize the Filtering Database window, a message will appear to inform you that data is being retrieved. The message will disappear when all information has been returned from the Filtering Database, and you will be able to view and configure database entries.

A scrollable Address Entry panel allows you to:

- View the address entries in the Filtering Database.
- Alter an entry's type (e.g., from Learned to Permanent, Dynamic, or Static).
- View and configure the bridging action taking place on the packets entering each of the bridging ports.

In addition, you can use buttons to add individual addresses to, or delete them from, these databases, or clear all Permanent, Static, or Dynamic entries in the database.

To access the Filtering Database window:

1. From the Bridge Status window, click on **Bridge** to display the Bridge Status menu.

or

From the Module View window, click on the **Bridge** label just above the port status display; the Bridge menu will appear.

2. Click on **Filtering Database....** The Filtering Database window will appear.

The following fields are listed in the top portion of the Filtering Database window:

List

The List checkboxes indicate whether the associated entry type (Permanent, Static, Dynamic, or Learned) will be displayed in the scrollable table of address entries. A check next to the entry type indicates that it will be displayed.

Type

Indicates the type of entry in the database.

Number

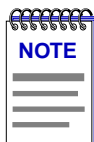
Displays the current number of Permanent, Static, Dynamic, and Learned Address entries.

Capacity

Indicates the total capacity of each entry type in the Static and Learned databases.

Ageing Time

Indicates the length of time, in minutes, that Dynamic and Learned Addresses in the Source Address Table are allowed to remain inactive before they are dropped from the database. The allowable time range for these entries is 10 to 1,000,000 seconds. Ageing time is not applicable to Static or Permanent entries. You can configure this field, as described in the next section.



Note that the Filtering Database Ageing Time is the same as the Ageing Time displayed (and configured) via the Port X Source Addresses window; setting the Ageing Time in the Filtering Database window also changes the time in the Source Addresses window, and vice versa.

The following fields are applicable to the scrollable Address Entry panel of Filtering Database entries.

Address

Lists the addresses for which the bridge's Filtering Database has forwarding and/or filtering information.

Type

Indicates the type of an entry in the database. The possible types are Static, Dynamic, Learned, Self, or Permanent. You can alter the entry type, as described in the next section.

Source Port

Indicates the index number of the port on which the address entry was first detected. A question mark (?) indicates that the address entry was not a learned entry, but Port Filtering information applies to it (i.e., the entry is a created Permanent, Dynamic, or Static entry and has corresponding filtering information).

Receive Port

Indicates the number of the port on which a frame must be received in order for the entry's Port Filtering information to apply. An asterisk (*) indicates that the receive port is promiscuous, and filtering parameters will be applied to all packets regardless of their source (assuming no conflicting entry applies). You can change the receive port, as described in the following section.

Port Filtering

Indicates the action that will take place at each bridge port when it receives frames from the selected address entry. A green arrow indicates that the frames received from the address will be forwarded to the port's associated segment (➔¹). A red circle indicates that frames will be filtered (blocked) from the port's associated segment (●²). You can change the Port Filtering action for Permanent, Static, and Dynamic entry types, as described in the next section. (Note that port filtering is scrollable among all the potential ports; however, only two consecutive ports can be viewed simultaneously.)

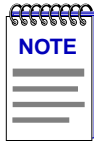
Configuring the Filtering Database

You can configure the Filtering Database by:

- Altering the Ageing Time for Dynamic and Learned entries.
- Changing the type of entry with the Type buttons.
- Changing the Receive port for the filter.
- Changing the Port Filtering action at each bridge port.
- Adding or deleting individual Filtering Database entries.
- Clearing all Permanent, Static, or Dynamic entries from the Filtering Database.

Note that although configuration changes will appear in the window, no action actually takes place in the bridge's Filtering Database until you click on in the bottom right of the window. This saves the new configuration. If you change the window without clicking , then attempt to exit the window by

clicking **Cancel**, a text box will appear stating “Changes have been made. Cancel them?”. Click on **Yes** to exit the window without changing the Filtering Database, or **No** to return to the window.

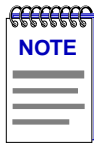


When you reconfigure the Filtering Database and click **OK**, the screen will clear temporarily and a message will appear to indicate that the information is being updated. When the changes have been successfully set and the Filtering Database has updated, the screen information will be refreshed.

Altering the Ageing Time

To alter the Ageing Time for Dynamic and Learned entries:

1. Highlight the **Ageing Time** field with the cursor.
2. Type in the new Ageing Time, in seconds; the allowable range is 10 to 1,000,000 seconds).



Note that the Filtering Database Ageing Time is the same as the Ageing Time displayed (and configured) via the Port X Source Addresses window; setting the Ageing Time in the Filtering Database window also changes the time in the Source Addresses window, and vice versa.

Changing the Type of Entry

You can change any entry type from its current type (Learned, Self, Permanent, Static, or Dynamic) to either a Permanent, Static, or Dynamic entry. To do so:

1. Click on the shadowed **Type** button. A menu will appear with the three possible types to which the entry can be changed.
2. Highlight the desired type.



If you wish to change the port filtering action for a Learned address entry, you must first change its entry type to Permanent, Static, or Dynamic.

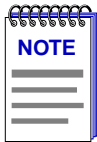
Changing the Receive Port

You can change the Receive port of an address entry in the scrollable panel, so that a frame must be received at the specified port for the filtering action to apply. To do so, click on the **Receive** port in the panel. With each click, the Receive port will cycle to the next port (e.g., from * (promiscuous), to 1, to 2, to 3, to 4, to 5, to 6 (etc., up to the total number of installed interfaces), and back to *).

Changing the Port Filtering Action

You can change the Port Filtering action at each bridge port from its current action to the opposing action.

1. Maneuver the scroll bar until the desired port is in the Port Filtering panel.
2. Click on the port to alter its filtering action from forwarding frames from the associated address (➔**1**), to filtering frames (●**2**) (or vice versa).



If you wish to change the port filtering action for a Learned address entry, you must first change its entry type to Permanent, Static, or Dynamic; note that when you do so, all Port Filtering action defaults to Blocking.

Adding or Deleting Individual Entries

You can add or delete entries individually from the Filtering Database.

To add an address:

1. Click on the **New** button in the lower left of the window. A window (Figure 5-6) will appear.

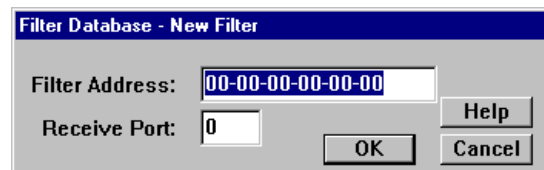


Figure 5-6. Filter Database – New Filter Window

2. In the **Filter Address** field, type in the MAC address (in hexadecimal format) for which you wish to configure forwarding or filtering parameters. Be sure to add “-” as a separator between each byte in the address.
3. In the **Receive Port** field, type in the port at which the address must be detected for bridging to take place. If you enter a value of 0 in this field, the Receive Port is considered promiscuous (i.e., any port), and will be designated by an * in the Address Entry panel.
4. Click on **OK**.
5. Specify the **Port Filtering** action on the address entry as described in the previous section.

To delete an address:

1. Click to highlight the address entry in the Address Entry panel that you wish to delete from the filtering database.
2. Click on **Delete**.

Clearing All Permanent, Static, or Dynamic Entries

To erase all Permanent, Static, or Dynamic entries from the Filtering Database, click on the associated **Clear** button in the upper portion of the window.

Configuring Duplex Modes

Any standard Ethernet interface on a 9H42x-xx module which is connected to another end station — i.e., another bridge interface — will support Duplex Mode operation. (Ethernet interfaces connected to repeaters will not support this mode.) Enabling Full Duplex mode on an interface allows the interface to receive and transmit packets at the same time, effectively doubling the available bandwidth (and, therefore, the wire speed) on the selected interface. Interfaces which are not set to Full Duplex mode must receive and transmit separately, waiting for one activity to be completed before the other is begun.



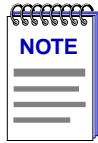
*For standard Ethernet interfaces, Full Duplex should **only** be enabled on an interface that has a connection to a single destination address at the other end of the connection (i.e., it is not a segment with an attached repeater cascading the connection to multiple destination addresses).*

Full Duplex mode disables the collision detection circuitry at the interface, so that both Transmit and Receive wires can be used simultaneously. With a single destination address at the other end of the connection (for example, if the connection was to a full duplex interface on another switching module, or if a single file server was connected to the full duplex switch port), this essentially doubles the available bandwidth from 10 Mbit/sec to 20 Mbit/sec. Note that the interface at the other end of the connection must also have Full Duplex enabled at the attached interface.

*Full Duplex mode **must** be disabled if the interface is communicating with multiple destinations simultaneously (i.e., if a repeater is cascaded from the interface), since Ethernet relies on Collision Sense for proper operation.*

You can configure the duplex mode for each appropriate interface via the Duplex Modes window accessible from both the Module View and Bridge Status window Bridge menus, and via the Port Configuration window accessible from both the Module View and Bridge Status window Port menus. From the Bridge menus, a single window allows you to both display and set the configuration of each

available standard Ethernet interface; windows accessed from the individual bridge port menus allow you to configure duplex mode operation for the selected interface only.



*For Fast Ethernet interfaces, you can set the duplex mode (along with additional parameters associated with auto-negotiation) via the Fast Ethernet Configuration window accessible from both the Module View and Bridge Status port menus. For more information on configuring duplex modes for both standard and Fast Ethernet interfaces at the port level, see **Chapter 2**. You cannot set the duplex mode for a Fast Ethernet interfaces from the Duplex Modes window described here.*

To access the Duplex Modes window:

1. From the Bridge Status window, click on **Bridge** to display the Bridge Status menu.

or

From the Module View window, click on the **Bridge** label just above the port status display; the Bridge menu will appear.

2. Click to select **Duplex Modes...**, and release. The Duplex Modes Window, [Figure 5-7](#), will appear.

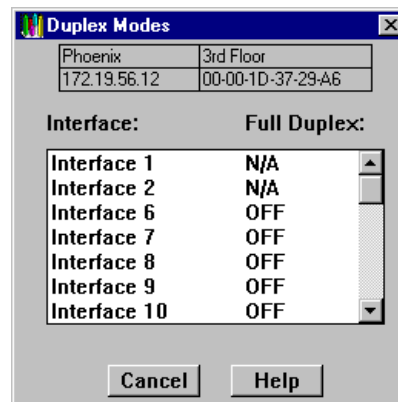


Figure 5-7. The Duplex Modes Window

The main portion of the Duplex Modes window consists of a list of interfaces available in the selected 9H42x-xx module and their current Full Duplex state: ON indicates that Full Duplex mode has been enabled for the selected interface; OFF indicates that it has not; N/A indicates that Full Duplex is either not available (for the INB interface) or cannot be set from this window (for Fast Ethernet interfaces).

To configure the Duplex Mode for any standard Ethernet interface:

1. In the Duplex Modes window, highlight the interface whose Duplex Mode you wish to change. Note that only one interface can be selected at a time.
2. Double-click the selected interface to toggle the Full Duplex setting from **ON** to **OFF**, or vice versa. The set will take place immediately.

Numerics

9H42x-xx devices described 1-1

A

absolute value 3-2, 3-12, 3-19
 accessing the RMON Alarm/Event list 3-11
 accessing the RMON Statistics window 4-1
 Accum 4-5
 Actions MIB 3-23
 Admin 2-9
 Admin/Link 2-9, 2-10
 Advanced Alarms 3-2
 Ageing Time (bridging) 5-19, 5-21
 Alarm Instance 3-16
 alarm log 3-5
 alarm status 3-12
 alarm threshold 3-1
 Alarms
 Advanced 3-2
 Basic 3-1
 Alarms Watch 3-12
 auto-negotiation 2-19, 5-26

B

Basic Alarms 3-1
 Blocking 5-5, 5-6
 Boot Prom, revision 2-4
 Bridge 2-9
 Bridge Mapping 2-9
 Bridge Menu 2-7
 Bridge Port Menu 2-8
 bridge port state 5-4
 Bridge Priority 5-13
 Bridge Protocol Data Units (BPDUs) 5-2, 5-11
 Bridge status mode 2-9
 Bridge Status window 5-3
 bridging interface status 5-4
 Broadcast/Multicast 3-4
 Broken 5-5
 buffer space 2-17, 4-8
 Bytes 4-3

C

Cancel button 1-6
 Collisions 4-4
 color-coded port display 2-2, 2-11
 command buttons 1-6
 community names 3-7
 in traps 3-7
 Connection Status 2-3
 CRC/Alignment 4-3
 creating and editing an advanced RMON alarm 3-14
 creating and editing an RMON event 3-20

D

data loops 5-5
 deleting an RMON alarm, event, or action 3-26
 delta values 3-2, 3-5, 3-7, 3-8, 3-12, 3-19, 4-2, 4-5
 Designated Bridge 5-11, 5-15
 Designated Cost 5-15
 Designated Port 5-11, 5-16
 Designated Root 5-15
 device date 2-26
 Device Menu 2-5
 Device Name 1-5
 device time 2-25
 Device Type 2-12
 devices described 1-1
 disable a bridge port 5-6
 Discarded packets 2-17, 4-8
 Drop Events 4-3
 duplex mode 2-19, 5-26
 Dynamic Ageing Time 5-19
 Dynamic entries 5-19

E

enable a bridge port 5-6
 event 3-1
 event index 3-13
 Event Log 3-13

Event Type 3-22
Events Watch 3-12, 3-13

F

falling action 3-5, 3-8
falling alarm threshold 3-1, 3-2, 3-5, 3-6, 3-8,
3-12, 3-18, 3-19
FallingEventIndex 3-19
Fast Ethernet Port Interface Module 1-1
Filtering Database 5-2, 5-19
flnNUcast 3-4
Firmware
 revisions supported 1-7
Firmware, revision 2-4
Forwarding 5-4, 5-6
Forwarding Delay 5-14
Fragments 4-4
Frame Size (Bytes) Packets 4-4
Frames Filtered 5-9
Frames Forwarded 5-8
Freeze Stats 4-6

G

Getting Help 1-6

H

Hello Time 5-14
Help button 1-6
Help Menu 2-7
Hold Time 5-14
how rising and falling (RMON) thresholds
 work 3-27
hysteresis 3-10, 3-27

I

I/F Summary window 2-13
 interface performance statistics 2-14
IF Number 3-4
IF Type 3-4
ifInErrors 3-4
ifInOctets 3-4
INB network bus 1-2
Interface Statistics window 2-16
interface type (bridging) 5-5
IP address 1-5, 2-3

J

Jabbers 4-4

K

Kilobits 3-4

L

L. Sta 2-14
Learned entries 5-19
Learning 5-5, 5-6
Listening 5-4, 5-6
Load 2-15
% Load 4-3
Location 1-5
Log Events 3-22
Log/Trap 3-5

M

MAC address 1-5, 2-4
Max Age 5-14
menu structure 2-4
MIB components 2-11
MIB II variables 3-4
MIBTree 3-16, 3-24
MMAC-Plus Chassis View 2-2
Module Type 2-12
Multicast (Non-Unicast) 2-17, 4-8

N

Non-Unicast (Multicast) 2-17, 4-8

O

OK button 1-6
Operational Modes 2-22
Operator 2-10
Oversized 4-4
Owner 3-15, 3-22

P

P. Sta 2-14
packet capture
 events 3-1
Packet Type 4-3
Packets 4-3
 Received 2-17, 4-8
 Transmitted 2-18, 4-8
Path Cost 5-15

peak values 4-2, 4-3, 4-4, 4-5
Permanent entries 5-19
Polling Interval 3-5
port configuration 5-26
port display, color codes 2-2
Port Filtering 5-22
Port Number 3-4
Port Status 2-3
 color codes 2-11
Port Status Display 2-8
Port Status Menu 2-6
Port Status Views 2-9
Priority 5-15
Problems 4-3
Protocol, bridging 5-14

R

Rate 2-15
Raw Counts 2-14
Receive Port 5-22
Remote Capabilities 2-23
rising action 3-5, 3-8
rising alarm threshold 3-1, 3-2, 3-5, 3-6, 3-7,
 3-12, 3-18, 3-19
RisingEventIndex 3-19
RMON alarm description 3-27
RMON Alarms and Events 3-1
Root Bridge 5-13
 selection process 5-11
Root bridge 5-11
Root Cost 5-13
Root Port 5-13

S

Sample Type 3-19
SecureFast Virtual Networking 1-2
SecureFast™ switching 1-2
Selecting Port Status Views 2-9
Set button 1-6
setting an RMON alarm variable 3-16, 3-24
Source Address Table 5-19
Source Port 5-22
Spanning Tree Algorithm (STA) 5-2
Startup Alarm 3-19
Static entries 5-19
Statistics (Ethernet) 4-2
Status (alarm) 3-5

T

Technical Support 1-7
threshold pairs 3-28
to change the status view of your ports 2-9
Topology Change 5-16
Total 4-5
Total Errors 3-4
% of Tot. Errors 4-4
traditional switching 1-2, 5-1
Transmit Queue Size 2-17, 4-8
transparent bridging 5-1, 5-19
Trap 3-22
Troubleshooting 2-17, 4-8

U

Undersized 4-4
Unicast 2-17, 4-8
Unknown Protocol 2-17, 4-8
Up Time 2-3, 2-13, 5-4
Utilities Menu 2-6

V

viewing an RMON event log 3-26

W

Web site 1-7

X

Xmitted 5-9

